Guide pour les utilisateurs d'Internet

Demoulin, Marie; Gobert, Didier; Lazaro, Christophe; Jacquemin, Hervé; Montero, Etienne

Publication date:
2003

Service public fédéral Economie,
PME, Classes moyennes et Energie

Guide pour les utilisateurs d'Internet

2003

Notes de l'éditeur

Remerciements

Le Service public fédéral Economie, PME, Classes moyennes et Energie remercie les auteurs de cet ouvrage.

Avertissement

La rédaction du présent ouvrage a été finalisée en novembre 2002. Aussi, nous attirons toute votre attention concernant les modifications éventuelles survenues depuis la rédaction dudit ouvrage, notamment des législations ou des tarifs. Nous attirons également votre attention sur le fait que ce guide est le résultat d'un travail de vulgarisation. Il ne dispense dès lors d'aucune manière de s'adresser à des conseillers techniques ou juridiques.

Traduction

La version d'origine de ce document a été écrite en français. La traduction en néerlandais a été assurée par le service de traduction du Service public fédéral Economie, PME, Classes moyennes et Energie.

Commande

Ce guide peut être consulté (en format html) ou télédéchargé (en format pdf) sur le site Internet du Service public fédéral Economie, PME, Classes moyennes et Energie :

Version en français :

http://mineco.fgov.be/information_society/consumers/consumers_internetguide/home_fr.htm

Version en néerlandais :

http://mineco.fgov.be/information_society/consumers/consumers_internetguide/home_nl.htm

Ce guide peut aussi être obtenu gratuitement par courrier, dans la mesure des stocks disponibles. Dans ce cas, veuillez envoyer votre demande au Service public fédéral Economie, PME, Classes moyennes et Energie en mentionnant le titre de l'ouvrage et votre adresse.

Service public fédéral Economie, PME, Classes moyennes et Energie
Statistique et Information économique
Rue de l'Industrie, 6 à 1000 Bruxelles

e-mail carrefour@mineco.fgov.be
http://mineco.fgov.be
tél. 02 506 51 11
fax 02 513 46 57

Editeur responsable

Hans D'HONDT, rue de Louvain 44, 1000 Bruxelles

Dépôt légal

D/2003/1226/08

Le présent Guide pour les utilisateurs d'Internet a été rédigé par le Centre de Recherches Informatique et Droit (FUNDP – Namur) dans le cadre d'un contrat de recherches financé par le Service public fédéral Economie, PME, Classes moyennes et Energie.

Auteurs :

Marie Demoulin
Didier Gobert
Christophe Lazaro
Étienne Montero

Sous la direction du Professeur Étienne Montero

Centre de Recherches Informatique et Droit
Facultés Universitaires Notre-Dame de la Paix
Rempart de la Vierge, 5
B - 5000 NAMUR

Tél. : 081/72.47.69.
Fax. : 081/72.52.02.

http://www.crid.be

Avant-propos

Ce guide a pour but de démystifier, dans un langage aussi clair que possible, l'environnement Internet et de répondre à la plupart des questions que VOUS, utilisateurs potentiels ou non, vous seriez amenés à vous poser.

En effet, que vous soyez profanes ou initiés, cet ouvrage vous permettra tantôt de vous familiariser avec une terminologie quelquefois mystérieuse tantôt d'optimaliser l'utilisation du média Internet.

Eu égard au nombre croissant d'utilisateurs et aux risques potentiels engendrés par ce nouveau média, le Service public fédéral Economie, PME, Classes moyennes et Energie, dans un souci de transparence, a demandé le concours du Centre de Recherches Informatique et Droit (CRID) des Facultés Notre-Dame de la Paix à Namur pour la réalisation du présent ouvrage.

D'entrée, ce guide aborde toutes les questions relatives à la mise en connexion sur Internet. Cette connexion réalisée, le guide envisage, dans un second temps, la consultation et la collecte de l'information sur le Net.

Qui dit Internet implique échange d'informations. Le guide en aborde toutes les facettes.

L'outil Internet étant multifonctionnel, ce guide vous sensibilise également aux achats sur Internet et à son corollaire le commerce électronique (e-commerce) dont l'avenir se révèle prometteur.

En outre, grâce à cette brochure, vous saurez tout de la conception d'un site 'Internet' ainsi que des 'plus' offerts par le vendeur.

Pour clore, le présent guide reprend dans un glossaire assez exhaustif l'ensemble de la terminologie propre à l'environnement Internet.

Bonne lecture !

Lambert VERJUS,
Président du Comité de Direction.

Table des matières

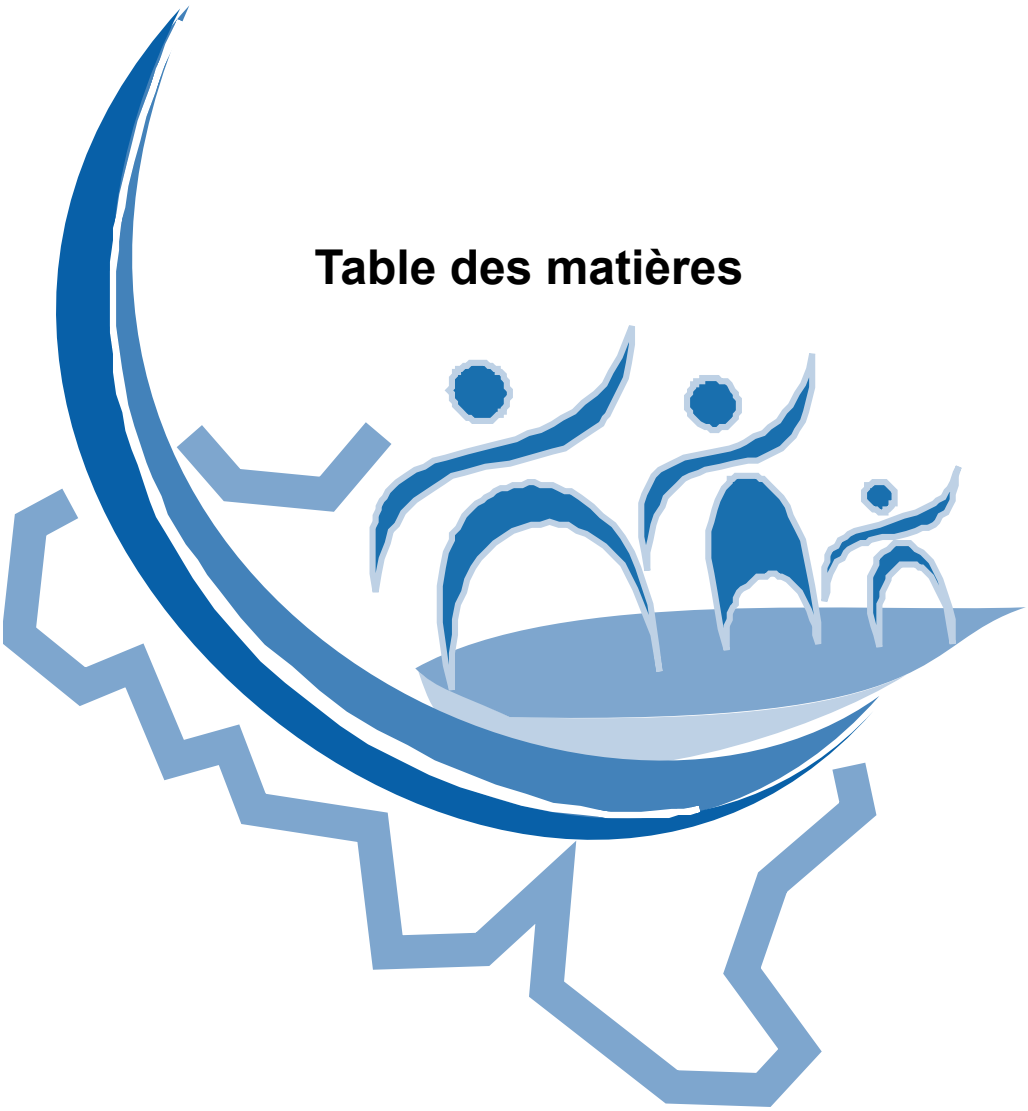
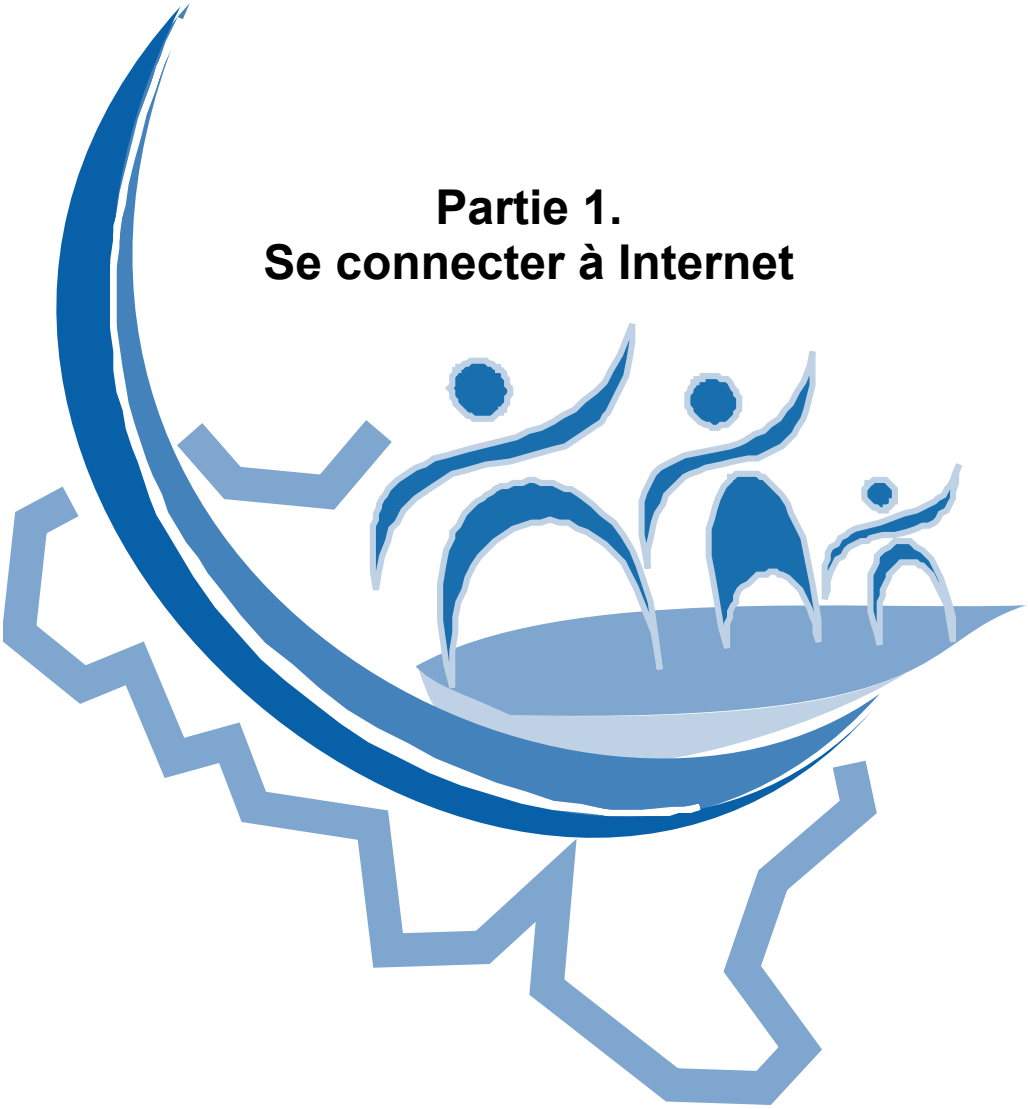


TABLE DES MATIERES

Partie 1.
Se connecter à Internet



CHAPITRE I. LA CONNEXION A INTERNET

Internet est devenu un moyen de communication permettant de rechercher et de consulter efficacement une variété inimaginable d'informations. Ce moyen de communication permet également d'entrer en contact ou de commercer avec une multitude de personnes, d'organisations, d'administrations et de commerçants situés aux quatre coins du monde.

Les relations qui peuvent se créer sur Internet dépendent de l'application utilisée. La consultation de sites web (qui peuvent contenir des informations sous forme de textes, d'images animées ou non, de sons, etc.) et l'envoi de courriers électroniques (accompagnés éventuellement d'un fichier attaché) sont les deux applications les plus fréquemment utilisées. A côté de celles-ci, il est également possible de participer à des forums de discussion (*newsgroup*), d'effectuer des discussions virtuelles en temps réel ("*chat*") ou encore de procéder à des transferts rapides de fichiers (*FTP*). De quelles clés ai-je besoin pour pouvoir accéder à ces merveilleuses possibilités ?

1. Quel est le coût de la connexion à Internet ?

Outre le prix de l'ordinateur ou du "boîtier interface", il convient d'additionner les éléments suivants (qui constituent des coûts fixes) :

Le prix du modem : modem RTC (*infra*, n° 4) à partir de 50,00 EUR, modem ADSL (*infra*, n° 7) à partir de 69,00 EUR, modem RNIS (*infra*, n° 5) à partir de 130,00 EUR, modem câble (*infra*, n° 6) à partir de 219,00 EUR.

L'abonnement aux fournisseurs d'accès Internet. Les fournisseurs d'accès offrent différentes formules d'abonnement à des prix très divers. Il convient de faire particulièrement attention aux tarifs appliqués en cas de connexion en dehors des périodes prévues dans le contrat. Depuis quelques années en Belgique, des accès à Internet sont offerts gratuitement (notamment : Belgacom.Net, TELonline, FreeWorld, Planet Internet, SwinG, Tiscali, etc.).

L'utilisateur prendra également en compte les éventuels **frais de communication** (qui constituent des frais variables en fonction de la durée et de la période de connexion ainsi que du type de technologie utilisée). Des tarifs spéciaux pour utilisateurs d'Internet sont appliqués (entre 1,00 EUR et 2,50 EUR l'heure, en fonction de la période de connexion). Des logiciels disponibles en ligne permettent de calculer les coûts de communication (on cite notamment : http://www.kri-soft.be/timer et http://www.timeupsoft.com).

2. Quel matériel et quels logiciels utiliser ?

Généralement, il est nécessaire de disposer d'un ordinateur pour pouvoir surfer sur Internet. L'ensemble des ordinateurs sur le marché permettent actuellement d'accéder à Internet. La configuration minimale est une vitesse de processeur d'au moins 100-120 MHz, 16 Mb de mémoire vive (RAM), et une carte graphique de 2 Mb. Il est toutefois beaucoup plus confortable de surfer sur Internet à partir d'une machine suffisamment puissante afin de ne pas devoir attendre indéfiniment l'apparition d'images ou d'autres animations.

Il n'y a aucune exclusivité sur le type d'ordinateur (PC ou MAC), ni sur le système d'exploitation nécessaire pour surfer sur Internet (Windows, Mac OS, Linux ou Unix).

Plusieurs logiciels sont nécessaires pour accéder aux différents services qu'offre Internet. Ils sont en général gratuits, offerts par le fournisseur d'accès Internet ou le vendeur de

matériel. Parmi les logiciels les plus répandus, on trouve *Outlook*, un logiciel de courrier électronique et *Internet Explorer* ou *Netscape Navigator,* utilisés pour surfer sur Internet. Mais ce ne sont pas les seuls. Il y en a de nombreux autres.

En effet, il faut savoir que, sur Internet, il est possible de télécharger un grand nombre de programmes destinés à des fins diverses. C'est le cas notamment sur les sites suivants : http://www.tucows.com, http://www.anshare.com et http://www.logicielscenter.com. Ces logiciels sont souvent gratuits. Parfois, ils sont gratuits dans une version de démonstration et payants par la suite. Soyez méfiant et ne téléchargez sur votre ordinateur que des logiciels dont vous êtes sûr de la source. Le risque existe de télécharger un virus (*infra*, n^{os} 108 et s.).

3. Quelle technologie de communication choisir ?

Différentes technologies sont actuellement offertes par les entreprises de télécommunication :

- le RTC (*infra*, n° 4) ;
- le RNIS (*infra*, n° 5) ;
- le câble de télévision (*infra*, n° 6) ;
- l'ADSL (*infra*, n° 7).

En ce qui concerne les "modems", pour chaque catégorie, il existe différentes normes, technologies et marques. Il est important de se faire conseiller par un professionnel lors de l'achat d'un tel bien.

4. Le Réseau Téléphonique Commuté (RTC)

De quoi s'agit-il ?

Le réseau téléphonique commuté est la ligne téléphonique traditionnelle. Cette technologie permet de transmettre des données à une vitesse théorique maximale de 56.000 bits par seconde. En pratique toutefois, le débit n'est pas toujours aussi rapide.

Cela répond-il à mes besoins ?

Actuellement, la ligne téléphonique classique est la plus utilisée par les particuliers pour surfer sur Internet. Elle est en règle générale déjà installée et ne nécessite pas l'intervention des services de télécommunication. Le système d'abonnement gratuit à Internet lié à l'utilisation d'une telle ligne fait que cette solution est la plus appropriée pour faire ses premiers pas et découvrir Internet moyennant un investissement minime. Elle a cependant deux principaux inconvénients. Premièrement, l'accès à Internet monopolise la ligne téléphonique (lorsqu'elle est activée) : il ne vous est plus possible de recevoir de coup de téléphone pendant que vous êtes connecté à Internet. Deuxièmement, le transfert de données est relativement lent. Or, les sites Internet délivrent des données de plus en plus volumineuses, ce qui rend parfois fastidieux le téléchargement des images, sons ou autres fichiers constituant les pages consultées.

Quel matériel dois-je acquérir ?

Si vous avez choisi de vous connecter à Internet via le réseau classique RTC, vous avez besoin d'un ordinateur et d'un modem. Le modem est généralement déjà installé sur votre ordinateur (n'hésitez toutefois pas à vous renseigner lors de l'achat). Il est cependant possible de l'acheter de façon séparée.

Pour les personnes qui n'ont pas les moyens ou qui ne souhaitent pas acquérir un ordinateur, un opérateur propose une solution alternative : la *Netbox.* Cette console simplifiée – moins onéreuse qu'un ordinateur – est reliée à la télévision équipée d'une prise péritel et à la ligne téléphonique classique. Elle donne accès à la plupart des services offerts sur Internet au prix d'une communication Internet classique. Ajoutons que dans la plupart des cas, il est nécessaire d'acheter en plus un clavier.

5. Le Réseau Numérique à Intégration de Services (RNIS)

De quoi s'agit-il ?

Le réseau numérique à intégration de services (RNIS ou ISDN, en anglais), est un réseau entièrement numérique qui offre un débit de transfert d'information caractérisé par sa rapidité et sa fluidité. Un accès de base met à votre disposition minimum deux canaux de 64.000 bits par seconde chacun. Si on utilise les deux lignes simultanément, cette technologie permet donc théoriquement de transmettre des données à la vitesse maximale de 128.000 bits par seconde dans les deux sens de la communication.

Cette technologie répond-elle à mes besoins ?

La liaison RNIS est plus stable et moins sensible aux perturbations analogiques que la liaison RTC. Elle est également plus rapide (on peut surfer jusqu'à quatre fois plus vite qu'avec une ligne classique). Elle permet donc un plus grand confort d'utilisation d'Internet. Cependant, l'inconvénient est que l'installation de cette ligne nécessite l'intervention payante d'une entreprise de télécommunication. Par ailleurs, l'utilisation de cette solution est plus coûteuse que l'usage de la ligne téléphonique classique, même s'il est vrai qu'elle vous permet, outre les avantages décrits ci-dessus, de surfer sur Internet et de téléphoner en même temps, car il y a deux canaux de communication. Toutefois, comme on le verra, l'ADSL apparaît plus intéressant que le RNIS pour le particulier qui veut surfer sur Internet. En effet, la vitesse de transmission est encore plus élevée et le prix est forfaitaire (et donc non lié à la durée de connexion).

Quel matériel dois-je acquérir ?

Pour surfer sur Internet à partir de la technologie RNIS, vous avez besoin d'une interface entre la ligne et votre ordinateur, appelé "modem RNIS".

6. Le câble de télévision

De quoi s'agit-il ?

Dans un nombre croissant de villes belges, des fournisseurs d'accès proposent un accès par le câble de télévision. Les vitesses atteintes par les modems câble sont largement supérieures à celles obtenues par un modem RTC. Toutefois, les vitesses de transmission dépendent fortement de l'heure de connexion et donc de l'occupation du réseau.

Cette technologie répond-elle à mes besoins ?

L'intérêt principal de cette technologie est d'apporter un réel confort dans l'utilisation d'Internet. Elle permet une connexion ultra rapide, 24h/24, sans interférer avec la télévision câblée. Toutefois, les vitesses de transmission peuvent fortement fluctuer suivant l'heure de connexion. Par ailleurs, elle ne fait pas appel à votre ligne téléphonique. Toutefois, la connexion au câble a pour inconvénient une grande rigidité. Si vous désirez utiliser Internet depuis différents endroits (avec un ordinateur portable), vous devez utiliser le modem classique, transportable aux quatre coins du monde.

Les frais sont forfaitaires, il n'y a plus de frais de communication téléphonique. Par contre, le coût du modem câble peut être plus important et l'abonnement auprès du fournisseur d'accès plus cher que celui des fournisseurs d'accès Internet classiques. Cette technologie est particulièrement adaptée aux personnes qui font une utilisation intensive d'Internet et qui téléchargent un volume important de données. Elle constitue une alternative intéressante à l'ADSL (*infra*, n° 7). Nous conseillons donc aux gros utilisateurs d'Internet de comparer attentivement ces deux technologies et les offres commerciales. Le câble est évidemment la solution idéale et unique pour les surfeurs qui ont pris la décision d'abandonner leur ligne classique au profit de leur GSM !

Attention, même si l'offre augmente de jour en jour, actuellement cette technologie n'est pas disponible sur tout le territoire belge. Ce service est notamment offert par Brutélé, tvc@blenet, Pandora (Telenet), Coditel, etc.

Quel matériel dois-je acquérir ?

Pour utiliser Internet par le câble, vous avez besoin d'un modem câble. Contrairement à leur dénomination, les modems câble ne sont pas comparables aux modems standard se connectant sur le réseau téléphonique commuté. Les différences sont assez conséquentes, tant au niveau de leur technologie intrinsèque, qu'au niveau de leurs performances. Le modem câble (externe) est généralement relié au PC via une simple carte Ethernet (que vous devrez éventuellement acheter si votre ordinateur n'en est pas équipé) par une fiche libre du PC.

7. L'ADSL

De quoi s'agit-il ?

La technologie ADSL (*Asymmetric Digital Subscriber Line*) permet, grâce à un modem de nouvelle génération, d'accroître les vitesses de transmission des données tout en utilisant votre ligne téléphonique classique (de l'ordre de 10 fois plus rapide pour le téléchargement de données et de 2 fois pour l'envoi de données). En effet, l'ADSL utilise la paire de câbles en cuivre traditionnel, le fil du téléphone, mais sur des fréquences plus élevées, ce qui permet de surfer et de rester connecté à Internet 24h/24 tout en laissant votre ligne téléphonique libre. A l'heure actuelle, en Belgique, les services ADSL sont offerts par Belgacom TurboLine. Cette technologie est très performante (1.000.000 bits par seconde du réseau vers votre ordinateur et 128.000 bits de votre ordinateur vers le réseau).

Cette technologie répond-elle à mes besoins ?

A l'instar du câble de télévision, l'ADSL est une solution réservée aux utilisateurs qui font un usage relativement important d'Internet. Actuellement, on peut globalement considérer que cette solution devient intéressante lorsque votre utilisation d'Internet via le RTC

dépasse les 30 heures de connexion par mois en heure creuse ou 15 heures par mois en heure de pointe.

Avec cette solution, vous payez un abonnement mensuel forfaitaire. Vous ne devez donc plus payer de frais de communication téléphonique liés à la durée de connexion. Par contre, il vous faudra – en plus de votre abonnement pour votre ligne classique – payer un abonnement pour votre ligne ADSL ainsi qu'un abonnement approprié auprès d'un fournisseur d'accès Internet.

Le prix forfaitaire de l'abonnement ADSL comprend généralement un volume maximal de transmission (allant de 10 à 15 Gygabytes par mois suivant les fournisseurs). Un supplément de prix est prévu en cas de dépassement de cette limite. Notez toutefois que pour un internaute moyen, ce volume sera en pratique très rarement atteint.

Indiquons qu'actuellement, pour des raisons techniques, seulement 90 % de la population peut bénéficier de l'ADSL, ce qui reste toutefois largement supérieur à l'accès à Internet par le câble de télévision. Nous vous conseillons donc de vous renseigner afin de déterminer si l'ADSL est accessible ou non dans votre région.

Quel matériel dois-je acquérir ?

Outre les filtres à installer sur les prises téléphoniques pour éviter les bruits, vous devez acquérir un modem ADSL. Ce matériel fait généralement l'objet d'un package et d'un prix global (allant de 100,00 à 250,00 EUR).

8. Tableau récapitulatif

(prix approximatifs au mois de septembre 2002)

	Ligne classique (RTC)	Ligne numérique (RNIS)	Câble	ADSL
Débit théorique en kbps (réception/ émission)	56/33,6	128/128	1000/128	1000/128
Type de facturation	A la durée	A la durée	Forfaitaire	Forfaitaire
Matériel nécessaire	Modem (± 50,00 EUR)	Modem (± 120,00 EUR)	"Modem câble" (± 200,00 EUR)	Modem ADSL (± 100,00 EUR)
Frais d'activation	En principe aucun car elle déjà installée dans la plupart des ménages	± 100,00 EUR	De 50,00 à 200,00 EUR	De 25,00 à 220,00 EUR
Abonnement mensuel	Pour la ligne analogique : 16,19 EUR	Pour les lignes numériques : 36,29EUR	A partir de 30,00 EUR	En plus de l'abonnement pour la ligne classique (16,19 EUR), abonnement ADSL : ± 30,00 EUR
Abonnement(s) mensuel(s) au fournisseur d'accès	De 0 à 15,00 EUR et plus	De 0 à 15,00 EUR et plus	Compris dans l'abonnement câble	± 8,00 à 10,00 EUR
Volume d'émission et de réception	Illimité	Illimité	Tarification supplémentaire si dépassement de la limite comprise dans l'abonnement	Tarification supplémentaire si dépassement de la limite comprise dans l'abonnement

Remarque : les prix indiqués sont susceptibles de modifications. Par ailleurs, il convient également de tenir compte des nombreuses offres promotionnelles proposées par les opérateurs.

CHAPITRE II. L'ACCES A INTERNET

9. Quels sont les éléments à prendre en compte pour choisir son fournisseur d'accès à Internet (FAI) ?

Afin de pouvoir utiliser Internet, vous devez nécessairement passer par un fournisseur d'accès à Internet (FAI). Pour ce faire, vous pouvez directement prendre contact avec l'un d'entre eux notamment par écrit, téléphone, téléfax et même par… Internet. Si vous optez pour une ligne RTC ou RNIS, le fournisseur d'accès vous enverra généralement un CD-Rom d'installation ainsi que la procédure de connexion et toutes les informations techniques nécessaires (comprenant entre autres le numéro de téléphone qui permettra à votre modem de se connecter au FAI). Pour les abonnements gratuits, il est fréquent que les CD-Rom d'installation soient distribués librement par le biais de magazines ou lors de l'achat d'un ordinateur. Vous recevrez également un nom d'utilisateur et un mot de passe permettant de vous identifier auprès de votre FAI. Chaque fois que vous vous connecterez à Internet, le modem composera le numéro de téléphone du FAI, il communiquera votre nom d'utilisateur et le mot de passe, qui permettront d' "ouvrir" une ligne entre vous et le FAI. Dès cet instant, vous pourrez surfer sur Internet ou consulter vos courriers électroniques par le biais des logiciels *ad hoc*. Si vous optez pour une ligne ADSL ou le câble de télévision, la procédure n'est pas bien différente. Néanmoins, l'installation nécessite parfois l'intervention d'un technicien si vous ne vous sentez pas de taille à la faire vous-même.

De nombreux fournisseurs d'accès existent sur le marché et ceux-ci proposent diverses formules d'abonnements, payants ou gratuits. En fonction de vos besoins, nous vous conseillons de comparer les différentes offres d'un même FAI ainsi que les offres de plusieurs FAI afin de déterminer la solution qui convient le mieux à vos desiderata et qui présente le meilleur rapport qualité/prix. Au-delà du prix, l'étendue des services offerts ne doit pas être négligée (vitesse de transmission, nombre d'adresses e-mail, espace pour héberger son propre site web, *helpdesk* payant ou gratuit, package "sécurité" compris ou pas, etc.).

Nous vous recommandons de lire attentivement les conditions d'abonnement insérées dans les contrats afin de déterminer quels sont vos droits et vos obligations. Un bon fournisseur d'accès met à votre disposition non seulement les conditions générales précitées, mais aussi un mode d'emploi contenant les informations techniques relatives à l'installation, le logiciel nécessaire pour la connexion et la navigation sur Internet, un service technique (*helpdesk*) personnalisé, une connexion de bonne qualité (vitesse élevée, faible taux d'erreur, peu de ruptures de connexion, etc.), un abonnement et un accès adaptés à vos besoins, une ou plusieurs adresses e-mail et un espace afin d'héberger vos propres pages web. Il doit également vous informer de sa politique concernant l'usage de vos données à caractère personnel.

L'ISPA (*Internet Service Providers Association*), association belge des fournisseurs d'accès à Internet, a élaboré un code de conduite que doivent respecter tous ses membres. Les fournisseurs d'accès sont libres de s'affilier à l'ISPA qui, bien que ne possédant pas le monopole de la bonne conduite, est certainement la principale référence en Belgique. Pratiquement, on constate que la grande majorité des FAI belges sont membres de l'ISPA.

Le code de conduite de l'ISPA – libellé il est vrai en des termes très généraux et peu contraignants – comprend les obligations suivantes :

- des obligations générales de légalité et de sincérité (les FAI veillent notamment à ce que leurs services et matériels de promotion ne prêtent pas à confusion) ;

- l'obligation d'honnêteté (à ce titre, les FAI doivent informer leurs clients de l'existence de ce code de conduite *et de la procédure de réclamation*) ;

- des obligations concernant la protection des données à caractère personnel (le code rappelle l'importance de veiller au respect de la loi – trop souvent ignorée – sur la protection des données à caractère personnel) ;

- un respect de la législation en matière de publicité (notamment dans le but d'éviter la publicité trompeuse et d'assurer une publicité comparative saine) ;

- des informations sur les prix (en vue d'éviter les ambiguïtés) ;

- des dispositions sur la criminalité ;

- une procédure de réclamation.

Selon ce code de conduite, vous pouvez porter plainte lorsqu'une des conditions de ce code n'est pas respectée par un fournisseur d'accès à Internet membre de l'ISPA. Vous pouvez soit adresser des réclamations au fournisseur d'accès, membre de l'ISPA, soit porter plainte directement auprès du comité ISPA. Si le comité de l'ISPA constate que la plainte est fondée et que le membre refuse de réagir aux injonctions du comité ou qu'il y a eu violation du code de manière répétitive, le membre peut être exclu de l'ISPA.

La liste des membres de l'ISPA ainsi que le code de conduite sont accessibles sur le site de l'ISPA : http://www.ispa.be.

10. Que penser de "Internet gratuit" ?

Les offres d'accès gratuit à Internet sont nombreuses. La formule est certainement idéale pour découvrir Internet, mais est-elle réellement gratuite ?

En premier lieu, si l'accès à Internet vous est fourni gratuitement, vous n'échappez pas à la nécessité de payer le prix de la communication téléphonique (ce qui suppose au préalable que vous ayez une ligne fixe), actuellement de 1,00 EUR par heure en heures creuses et de 2,50 EUR par heure en heures de pointe, auquel il faut ajouter le coût de connexion de 0,05 EUR. Par ailleurs, vous devez nécessairement disposer d'un ordinateur équipé d'un modem ou à tout le moins de la *Netbox* (moins onéreuse qu'un ordinateur) que vous pouvez relier à votre téléviseur, pour autant qu'il soit équipé d'une prise péritel.

Ensuite, l'accès à Internet vous est souvent proposé à l'achat d'un produit ou d'un service payant (ouverture d'un compte à vue, achat d'un ordinateur, etc.). Il arrive également que l'utilisateur s'engage à recevoir de la publicité. Les techniques de marketing se révèlent souvent plus agressives lors de telles offres et comportent de nombreux risques d'atteinte à la vie privée. Soyez donc conscient des effets secondaires liés à l'offre gratuite.

Enfin, la qualité de la connexion n'est pas toujours garantie à un niveau équivalent à celui d'un abonnement payant. La connexion risque de se révéler moins rapide ou de se trouver bloquée (la ligne est occupée). De plus, l'aide en ligne pour obtenir des conseils commerciaux et/ou techniques pour l'installation ou l'utilisation (*helpdesk*) est parfois payante.

En conclusion, la formule d'accès gratuit est certainement la solution idéale pour faire ses premiers pas sur Internet et pour les utilisateurs qui font un usage très occasionnel d'Internet. Mais il y a de bons accès gratuits à Internet et d'autres où la gratuité réserve certaines surprises. Pour ces derniers, vous devez déterminer si vous êtes prêt à supporter les quelques contraintes qui conditionnent l'accès gratuit à Internet.

11. Ma vie privée est-elle respectée ?

Lorsque vous souscrivez à un abonnement – gratuit ou payant – auprès d'un fournisseur d'accès à Internet, il vous est demandé de remplir un formulaire et d'inscrire certaines données qui peuvent être qualifiées de données à caractère personnel. Une donnée à caractère personnel est une information relative à une personne physique qui l'identifie ou qui permet – directement ou indirectement (par le recoupement avec d'autres informations) – de l'identifier.

Le fait que le FAI collecte des données n'est pas critiquable et est même indispensable pour pouvoir répondre efficacement à votre demande. Toutefois, la quantité et le type de données collectées peuvent parfois paraître excessifs voire déplacés au regard de la demande faite (obtenir uniquement un accès à Internet) : il en est ainsi lorsqu'on vous demande votre sexe, votre profession, votre rémunération, vos centres d'intérêts, vos principaux loisirs, etc.

Sachez que la collecte et plus généralement le traitement de données à caractère personnel est entouré de nombreux garde-fous consacrés par la loi sur la protection de la vie privée (*infra*, n^{os} 72 et s.). Celle-ci vous reconnaît notamment des droits tels que le droit à une information préalable complète, le droit d'accès aux données vous concernant, éventuellement assorti du droit de faire rectifier, voire supprimer, tout ou partie de ces données, ainsi que le droit de vous opposer à certains traitements illégitimes ou au traitement de vos données à des fins de marketing direct.

12. Quelles sont mes obligations envers le fournisseur d'accès à Internet ?

En règle générale, vous n'aurez pas la possibilité de négocier votre contrat avec votre fournisseur d'accès Internet. Il s'agit d'un contrat d'adhésion qui se présente d'ordinaire comme "à prendre ou à laisser". En cas de litige, cette situation devrait toutefois conduire à une interprétation du contrat en votre faveur par le juge.

Bien évidemment, ce n'est pas parce que vous n'avez pas eu la possibilité de négocier le contrat avec votre fournisseur d'accès à Internet que vous n'êtes pas tenu de respecter les clauses de celui-ci (pour autant que vous ayez été en mesure d'en prendre connaissance et de les accepter). En général, le contrat prévoit notamment que le client doit :

- se conformer aux exigences techniques précisées ;
- se conformer aux règles en usage sur le réseau ;
- se conformer aux lois et obligations en vigueur ;
- payer le prix.

Bien souvent, le fournisseur d'accès y ajoute certaines clauses précisant les obligations de l'utilisateur (par exemple, l'interdiction de créer des liens vers des fichiers MP3 illicites ou l'interdiction d'héberger sur son site web du contenu illégal ou préjudiciable). Vous êtes

tenu de respecter ces clauses car le contrat a valeur de loi entre vous et le fournisseur d'accès.

Cependant, il existe plusieurs limites à ce principe. Tout d'abord, certaines clauses sont parfois tout simplement illégales car elles violent une disposition légale impérative. Elles peuvent à ce titre être invalidées. Par ailleurs, certaines clauses limitatives ou exonératoires de responsabilité dépassent les limites développées par la jurisprudence et peuvent aussi être sanctionnées par le juge. Enfin, la loi sur les pratiques du commerce et la protection du consommateur vous protège contre les clauses abusives, c'est-à-dire contre les clauses qui créent un déséquilibre manifeste entre les droits et obligations des parties. Les clauses abusives sont interdites, spécialement si elles sont défavorables au consommateur, et donc considérées comme nulles. En pratique, il faudra analyser les clauses au cas par cas afin d'évaluer si elles sont abusives.

13. Quelles sont les clauses abusives parfois contenues dans les contrats des fournisseurs d'accès à Internet ?

Comme expliqué précédemment, une clause abusive est une clause du contrat qui provoque un déséquilibre manifeste entre les droits et obligations des parties. En pratique, il appartient au juge d'apprécier si la clause est réellement abusive et dans ce cas, il l'annulera.

Toutefois, le pouvoir d'appréciation du juge est parfois largement guidé par la loi. En effet, l'article 32 de la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur consacre une liste concrète de clauses qui sont considérées comme abusives, et donc interdites et nulles. En voici quelques-unes provenant de contrats de certains fournisseurs d'accès à Internet :

- "Le FAI se réserve le droit de modifier le prix à tout moment".

  La loi dit que le vendeur ne peut faire varier le prix en fonction d'éléments dépendant de sa seule volonté ;

- "L'abonné ne pourra pas demander la résolution du contrat dans l'hypothèse où le FAI ne fournit pas ses services pour des raisons de force majeure ou toute autre raison".

  La loi dit que le vendeur ne peut vous interdire de demander la résolution du contrat dans le cas où il n'exécute pas ses obligations ;

- "Le FAI se réserve le droit de résilier le contrat, sans préavis ni indemnité, en cas d'absence de connexion au service pendant une durée consécutive égale ou supérieure à un mois, en cas de cessation de l'exploitation du service… ".

  La loi dit que le FAI ne peut rompre ou modifier le contrat unilatéralement, sans vous dédommager, hormis le cas de force majeure ;

- "Le FAI n'est pas responsable des dommages en cas de perte de données informatiques stockées sur son propre système, ou autres dommages résultant de ses services …".

  La loi dit que le FAI est au moins responsable s'il y a eu une faute intentionnelle ou une faute grave de lui ou de ses employés ;

- “L’abonné reconnaît expressément que toute communication faite au FAI par e-mail a la même valeur qu’un écrit. Tout message envoyé à l’aide de l’adresse e-mail ou alias de l’abonné est réputé émaner de l’abonné qui s’engage à en assumer toutes les conséquences”.

  La loi dit que le FAI ne peut limiter les moyens de preuve que le consommateur peut utiliser ;

- “L’abonné renonce, en cas de conflit, à tout recours contre le FAI”.

  La loi dit que le FAI ne peut obliger le consommateur à renoncer à tout moyen de recours contre lui.

Partie 2.
Communiquer sur Internet

CHAPITRE I. CONSULTER DE L'INFORMATION

Section 1. Le cheminement de l'information sur Internet

14. Quel est le trajet suivi par l'information envoyée sur Internet ?

Internet est souvent surnommé "le réseau des réseaux". Cette description est relativement proche de la réalité. En effet, Internet repose sur une architecture technique composée d'ordinateurs, de logiciels, de routeurs ... Toutes ces machines sont reliées les unes avec les autres, grâce au maillage mondial des lignes de communication. Mais surtout, une communication entre les ordinateurs de ce gigantesque réseau est rendue possible par l'usage d'un standard de communication : le protocole TCP/IP. Ce protocole est la partie la plus fondamentale d'Internet puisqu'il constitue une sorte de "langage universel" de communication informatique.

Lorsqu'une machine désire communiquer avec une autre, elle envoie l'information en la découpant sous forme de paquets (paquets IP). Chaque paquet suit un cheminement à travers le réseau Internet, en utilisant les liaisons informatiques les moins chargées de manière à optimiser le temps de transmission. A l'arrivée, les paquets sont naturellement reconstitués. Des outils techniques permettent de connaître le chemin que parcourent les données pour arriver à destination. Contrairement à ce que l'on croit, les données n'empruntent pas nécessairement le chemin le plus court. En effet, elles suivront les chemins les moins encombrés. Même si elles concernent deux acteurs belges, les données peuvent aussi passer par l'Italie, la France, la Norvège, les Etats-Unis, etc.

Concrètement, ce protocole fonctionne selon le modèle requête/réponse. Votre navigateur demande une page Internet (*requête*) et le serveur interrogé répond à cette demande (*réponse*).

Vous introduisez un nom de domaine dans votre navigateur (par exemple : http://www.droit.fundp.ac.be). Cette adresse est traduite en chiffres, on appelle ça *l'adresse IP* (138.48.9.6 par exemple). En tapant sur la touche ENTER, votre requête est envoyée à votre fournisseur d'accès à Internet qui l'envoie à son tour dans le réseau Internet.

A l'intérieur de ce réseau, il existe à chaque "carrefour" un ordinateur appelé "routeur" qui, sur la base de l'adresse IP, envoie votre requête dans telle ou telle direction. Lorsque votre requête est arrivée sur l'ordinateur de réception appelé serveur, celui-ci renvoie en réponse ce que vous avez demandé. La réponse est, elle aussi, envoyée sur le réseau pour arriver à votre ordinateur ou à votre boîte aux lettres électronique.

15. Qu'est-ce que le "cache" sur le disque dur ?

Pour l'application Internet, le "cache" est l'espace sur le disque dur et dans la mémoire vive (RAM) de votre ordinateur où votre navigateur enregistre les copies des pages web consultées récemment. Votre navigateur se sert du cache comme mémoire à court terme.

L'**avantage** du cache est que votre ordinateur, reconnaissant votre demande, ne va pas télécharger l'information (l'image sur le site web que vous avez visité récemment) sur le réseau, mais il va charger l'image enregistrée dans votre dossier "cache", ce qui accélère considérablement la navigation.

L'**inconvénient** est que le contenu de certaines pages web est régulièrement mis à jour. Aussi, si une page est enregistrée dans votre cache, elle vous apparaîtra telle qu'elle y a

été enregistrée lors de votre dernière consultation, sans tenir compte des éventuelles mises à jour. Pour avoir la dernière version de la page, vous devez demander au navigateur d'actualiser la page. Un autre inconvénient, c'est qu'il est possible pour un utilisateur averti d'avoir accès à cette mémoire cache et de visualiser les pages qui ont été visitées par l'internaute précédent sur le même ordinateur.

Si vous le désirez, vous pouvez vider le cache, c'est-à-dire supprimer tous les fichiers que le cache contient lorsque ces fichiers commencent à occuper trop d'espace sur votre disque dur, ou lorsqu'ils sont périmés et ne correspondent plus aux fichiers sur le serveur web. Vous pouvez également modifier la taille du cache. Vous pouvez le réduire si vous avez besoin d'espace sur votre disque dur ou l'accroître si vous disposez d'un important espace disque. Un cache plus volumineux signifie que vous pouvez consulter plus rapidement un plus grand nombre de pages récentes. Toutefois, un cache trop volumineux ne constitue pas nécessairement un avantage. En effet, votre ordinateur pourrait alors mettre plus de temps à chercher dans les fichiers contenus dans le cache que pour effectuer une recherche sur Internet.

Sachez qu'à une autre échelle, les fournisseurs d'accès à Internet utilisent aussi une mémoire cache. Cette situation comporte les mêmes avantages et inconvénients que le cache de votre ordinateur. Lors de votre abonnement au fournisseur d'accès Internet (FAI), vous pouvez demander au FAI de ne pas vous fournir les pages web venant de son propre "cache". Cela peut éventuellement augmenter le prix de votre abonnement.

Section 2. La recherche de l'information sur Internet

16. Qu'est-ce qu'une URL ?

On appelle URL (*Uniform Resource Locator*) les adresses des différents éléments accessibles d'Internet. Chaque élément présent sur Internet possède en effet sa propre adresse, même s'il s'agit d'une simple image graphique sur une page web. Les adresses auxquelles vous avez le plus souvent affaire sont des adresses de niveau supérieur ; il s'agit, par exemple, des adresses qui permettent d'accéder aux pages d'accueil des sites web.

L'URL de la plupart des sites web mentionne, après l'identification du protocole (par exemple : http, pour *Hypertext Transfer Protocol*), les lettres www. Concrètement, ces trois lettres indiquent que la voie d'accès est le *World Wide Web*, c'est-à-dire le standard adopté dans Internet pour pouvoir accéder facilement à n'importe quelle ressource du réseau.

Il est utile, pour une navigation plus facile, d'archiver dans votre navigateur les adresses Internet (URL) que vous jugez intéressantes afin de ne pas devoir les retaper chaque fois que vous souhaitez y accéder. Les navigateurs de Microsoft et de Netscape rendent cette tâche très simple et conservent les adresses dans des dossiers désignés sous le nom de "favoris" par Internet Explorer et de "signets" par Netscape Navigator. Une fois archivées, il suffit de les sélectionner dans une liste et de cliquer dessus.

17. Qu'est-ce qu'un moteur de recherche ?

La meilleure manière de retrouver son chemin sur Internet reste l'utilisation d'un service spécifique appelé "moteur de recherche".

En fait, si vous savez déjà où aller sur le web et que vous connaissez l'adresse du site, saisissez-la directement dans le navigateur. Si, au contraire, vous êtes à la recherche d'un site particulier dont vous ne connaissez pas l'adresse ou si vous vous posez une question

sur un sujet spécifique, vous devrez d'abord découvrir l'adresse du site qui correspond à vos attentes. Les moteurs de recherche sont conçus pour retrouver des adresses de sites à partir des renseignements que vous saisissez.

Un moteur de recherche utilise un logiciel d'exploration, appelé "robot", qui visite en continu les pages web et les indexe de manière automatique dans une base de données, en fonction des mots-clés qu'elles contiennent. Lorsqu'une recherche est effectuée sur le site du moteur de recherche par la soumission d'un ou plusieurs mots-clés, le site affiche en réponse une série de documents "hypertextualisés". Pour chaque document sélectionné, un "score de pertinence" est établi, qui fait intervenir la fréquence d'occurrence des mots significatifs de la requête dans le document, leur proximité entre eux, leur présence dans le titre du document, etc. Les facteurs qui influent sur le référencement dans les moteurs de recherche peuvent être multiples, les plus importants étant la présence des mots-clés dans l'URL, c'est-à-dire l'adresse du site, dans le titre et le premier sous-titre ou paragraphe du site, ainsi que dans les métatags.

Les métatags sont des mots cachés insérés dans les codes HTML d'un site. Les principaux moteurs de recherche utilisent ces métatags pour indexer les sites qu'ils répertorient. Ainsi, si le propriétaire d'un site de vente de voitures de luxe souhaite que ses pages web soient référencées sous les mots-clés "vente voiture luxe" par les moteurs de recherche reconnaissant les métatags, il lui suffira d'insérer ces mots dans ses codes HTML.

Il existe un grand nombre de moteurs de recherche. Tous ne fonctionnent pas exactement de la même manière. Certains moteurs tentent d'être exhaustifs, tandis que d'autres ne référencent que les meilleurs sites. Parmi les moteurs de recherche les plus connus, on peut citer Google, AltaVista, Advalvas, Lycos, Infoseek, etc.

Le problème dans l'utilisation d'un seul moteur réside dans le fait que l'on n'est pas sûr d'obtenir une réponse à la question posée. En effet, il suffit que le moteur n'ait pas référencé le site demandé pour que l'on n'obtienne pas de réponse. Si vous utilisez un métamoteur (exemple http://www.copernic.com/), il y a peu de chance que ce désagrément arrive. En effet, un métamoteur utilise un logiciel permettant l'accès simultané à plusieurs moteurs de recherche. Vous aurez donc forcément au moins une réponse à votre question. Le seul inconvénient que l'on peut trouver à l'utilisation d'un métamoteur est qu'il peut y avoir trop de réponses... Dès lors, tout dépendra du choix des mots-clés que vous introduisez. Il faudra donc veiller à faire une recherche affinée, sur la base de mots-clés précis, de manière à ne pas être submergé de réponses.

Enfin, à côté des moteurs de recherche "généralistes", qui explorent et indexent tous les sites du réseau sans distinction et qui sont généralement intégrés à des portails "grand public", de plus en plus de moteurs spécialisés font leur apparition (recherche de contenus juridiques, d'articles de presse en ligne, de fichiers MP3, d'images et photographies, de séquences vidéo, etc.).

18. Comment mon site peut-il être référencé par un moteur de recherche ?

Il existe deux solutions.

Vous pouvez déclarer vous-même votre site ou votre page : lors de la mise en ligne de pages ou d'un site web, mieux vaut référencer ce site vous-même dans les moteurs de recherche souhaités. Pour cela, il suffit généralement d'aller sur le site du moteur de recherche et de cliquer sur le lien vous proposant de l'aide ou des informations concernant cette déclaration. Vous y êtes alors guidé.

Vous pouvez aussi attendre que cela se fasse automatiquement : des “robots” (logiciels appelés butineurs, *crawlers* ou *spiders*) scrutent le réseau, vont de page en page (en fait, de lien en lien) et sauvegardent au fur et à mesure le contenu-texte des pages rencontrées, constituant ainsi un “index”. Par exemple, AltaVista stocke 350 millions de pages. Le robot repasse périodiquement sur les pages qu’il a déjà indexées pour mettre à jour sa base d’informations.

19. Qu’est-ce qu’un annuaire ?

Les annuaires ou répertoires sont des listes de sites organisées en catégories et sous-catégories. Pour figurer dans la base de données, un site doit préalablement s’enregistrer par le biais d’un formulaire, indiquant un titre, une courte description et des mots-clés relatifs au document. Il ne s’agit donc pas d’une indexation automatique effectuée par un “robot”, mais d’un référencement humain et “volontaire”, sollicité par le titulaire du site lui-même, et traité “manuellement” par l’annuaire. De nombreux répertoires proposent également des “robots”, permettant une recherche par mots-clés dans les sites repris dans l’annuaire ou sur tout le web, voire les deux.

20. Qu’est-ce qu’un lien hypertexte ?

La navigation sur Internet se fait grâce aux liens hypertextes. Cette technique est là pour aider l’utilisateur à trouver, par renvois successifs, l’information qu’il désire et permet donc de surmonter l’incroyable dispersion de l’information disponible sur Internet.

Les liens hypertextes (ou “pointeurs”, ou “hyperliens”) sont généralement des mots soulignés en bleu (ou, en tout cas, dans une couleur différente de celle utilisée pour le texte principal). Parfois, ils sont représentés par une image (fixe ou animée : un logo, un bouton-pressoir, un *java script*, etc.). Lorsque l’on clique sur un lien hypertexte, on accède à une autre page web. Chaque lien hypertexte est relié à une autre page ou à un document multimédia qui a sa propre adresse URL. En cliquant sur ce lien, relié à une adresse, on donne un ordre à un serveur qui contient cette page. Un lien hypertexte est une indication interactive des coordonnées d’une page web, d’une image ou d’un espace bien précis à l’intérieur d’un document numérique. L’indication va permettre d’être directement lié au document qui fait l’objet du lien hypertexte en cliquant simplement sur le texte ou l’image qui se réfère à ce document.

Le lien hypertexte comporte deux aspects : l’un visible, l’autre caché. L’élément visible est l’intitulé que le concepteur de la page veut lui donner ; il ne sert que d’information visuelle. L’élément caché est l’adresse URL. L’intitulé peut cependant être l’adresse URL de la page à laquelle l’hyperlien renvoie.

21. Quels sont les différents types de liens hypertextes ?

- Le lien HREF : il s’agit du lien qui renvoie un document vers un autre par affichage sur le navigateur d’un tout nouvel écran.

  Une distinction subsidiaire existe cependant entre “lien hypertexte simple” (ou *surface linking*) et “lien hypertexte profond” (ou *deep linking*). Le premier établit un lien vers la page d’accueil (*homepage*) d’un site web, tandis que le second établit un lien vers une page secondaire d’un site web, c’est-à-dire toute page web différente de la page d’accueil.

- L’insertion par hyperlien (*inlining*) : ce type d’hyperlien permet l’insertion, dans une page web, d’une image (un graphique, un logo, etc.) provenant d’une autre page web

(appartenant au site web visité ou à un autre site) sans quitter la page web que l'on est en train de visiter.

Cette technique peut donner l'impression de visualiser une image provenant de la page web consultée alors que l'image provient en fait d'un autre site web. En effet, l'image ainsi incluse dans la page web est située sur le serveur d'un autre site web. Dès lors, ce lien donne la possibilité d'insérer sur un site web des images situées sur d'autres sites, sans devoir les copier, ce qui permet d'utiliser moins d'espace sur le disque dur du serveur qui héberge le site.

– Le cadrage (ou *framing*) : cette technique permet d'afficher une page ou un contenu provenant d'un autre site (site source) dans sa propre page web (site cible), sans passer par l'ouverture d'une nouvelle fenêtre du navigateur renvoyant au site source. L'adresse du site cible est donc substituée à celle du site source, ce qui donne la fausse impression que le contenu en question est celui du site cible (*infra*, n° 59).

  Avec ce type de lien hypertexte, l'adresse URL de la page qui pratique le cadrage ne change pas, même si c'est la page d'un autre site web qui est visitée.

CHAPITRE II. COLLECTER DES INFORMATIONS

22. Peut-on tout télécharger sur Internet ?

Internet est un réservoir constamment approvisionné de textes, d'images (dessins, photos, logos, graphiques), de fichiers musicaux ou vidéos, de logiciels, etc. Il est même possible de se procurer un film complet sur Internet si on fait preuve de patience et que l'on dispose d'une connexion rapide, ce qui est de plus en plus fréquent avec l'ADSL ou l'abonnement au câble. D'un point de vue technique, ces différents fichiers peuvent très aisément être copiés, téléchargés et réutilisés. Est-ce à dire que, d'un point de vue juridique, on peut tout télécharger sur Internet ? Non, en aucun cas !

Internet n'est pas un self-service gratuit, dans lequel on peut prendre et faire tout et n'importe quoi. Comme dans le monde traditionnel, certaines règles ainsi que les droits d'autrui doivent être respectés. En d'autres mots, la liberté des uns s'arrête là où commence celle des autres. Parmi les principales contraintes dont l'internaute doit tenir compte, figurent les droits de l'auteur de l'information que l'on se propose de copier, télécharger et/ou de réutiliser. Ces contraintes jouent bien entendu dans les deux sens : elles limitent le surfeur lorsqu'il veut télécharger ou exploiter certaines informations, mais à l'inverse, elles le protègent s'il devient lui-même un acteur actif, par exemple, l'auteur d'un texte original ou d'une image, voire le créateur d'un site web complet qui devient lui-même protégé.

Dans ce cadre, il convient de se poser diverses questions avant d'agir, telles que : quels sont les éléments protégés par le droit d'auteur ? quels sont les droits de l'auteur ? ne puis-je jamais reproduire une œuvre protégée par le droit d'auteur ? comment puis-je obtenir une autorisation auprès de l'auteur ? puis-je scanner une photo ou un texte pour le mettre sur mon site ? puis-je placer des fichiers musicaux (MP3 par exemple) sur mon site ? puis-je utiliser sans crainte un logiciel prétendu "*freeware*" ou "*shareware*" ? etc.

Par souci de cohérence, ces questions seront traitées dans la partie "Concevoir mon site web" (*infra*, n^{os} 42 et s.).

CHAPITRE III. ECHANGER DES INFORMATIONS

Section 1. Le courrier électronique

23. Qu'est-ce que le courrier électronique ?

Le courrier électronique (ou e-mail, courriel) peut être défini comme tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public de communications et qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère.

Concrètement, le courrier électronique vous permet d'envoyer immédiatement des messages à tout utilisateur d'Internet possédant une adresse électronique. Le message envoyé est composé de deux parties : l'en-tête et le corps du message. Des fichiers (ou attachements) peuvent être joints au message : ils peuvent contenir tant du texte que des images ou du son.

Il y a deux principaux services de courrier électronique. Le premier est assuré par le fournisseur d'accès : celui-ci attribue une adresse électronique et assure l'acheminement sur le réseau. Le traitement des messages se fait sur le poste de l'expéditeur, grâce à un logiciel de courrier. Les logiciels de courrier électronique les plus fréquemment utilisés sont Microsoft Outlook, Eudora et Nestcape Messenger. Le second type de service, le courrier web, est accessible à partir d'un logiciel de navigation qui autorise l'envoi et la réception du courrier par un ordinateur relié à Internet, indépendamment d'un fournisseur d'accès. Tel est le cas, par exemple, des services de messagerie gratuits comme *hotmail*, *caramail*, *wanadoo*, etc.

La notion de courrier électronique recouvre également l'utilisation du "chat", de la vidéoconférence ou l'envoi de message SMS (*Short Message Systems*) à partir d'un téléphone mobile. Il peut encore s'agir de messages laissés sur répondeurs téléphoniques ou sur "boîtes vocales" de téléphones mobiles.

24. Quels sont les faiblesses du courrier électronique ?

L'un des premiers problèmes liés au courrier électronique tient au maintien de l'intégrité et de la confidentialité de son contenu. En effet, de par sa conception, le courrier électronique n'est pas vraiment sécurisé. En transitant "à découvert" d'un ordinateur à l'autre, le courrier envoyé peut être intercepté, consulté, voire modifié par un utilisateur mal intentionné. Ce dernier peut en outre, communiquer un message reçu à une liste de diffusion ou à un forum de discussion (sous couvert, pour le diffuseur, de l'anonymat). Peuvent alors en découler tous les risques liés aux communications publiques : diffamation, atteinte à la vie privée, etc.

Les mots de passe attribués à votre compte de messagerie créent une illusion d'intimité, alors qu'en réalité, le courrier électronique offre à peu près le même degré de confidentialité qu'une carte postale. Le danger, toutefois, est *relatif*. En effet, qu'un inconnu lise vos mails courants n'est pas bien grave. Il faut bien reconnaître que l'essentiel de nos messages ne revêt sans doute pas un grand intérêt pour d'éventuels espions. Il peut toutefois arriver que le secret soit primordial : négociations d'affaires, échanges d'ordre strictement privé, etc.

Pour remédier à ce problème, il existe deux solutions cumulables : l' "anonymisation" du message et son chiffrement (cryptage). La première technique offre, comme son nom l'indique, la possibilité pour l'expéditeur de rester dans l'anonymat.

La seconde technique a pour but de ne rendre un message lisible que par les personnes "autorisées", c'est-à-dire celles qui possèdent la clé permettant d'avoir accès à son contenu. Ainsi, grâce aux nouveaux systèmes de cryptage, le courrier électronique peut maintenant être considéré comme une solution appropriée pour transmettre une information hautement confidentielle. Cependant, bien que le cryptage des données offre une bonne protection et soit un moyen sécurisé d'authentification de l'expéditeur, il occasionne d'autres problèmes puisqu'un message dont on a perdu la clé de (dé)chiffrement peut parfois être considéré comme perdu. En fait, vous ne devriez avoir recours à ce type de protection que dans des cas bien précis où vous estimez que le secret s'impose vraiment. Si vous n'avez jamais eu le sentiment d'avoir quelque chose de très important à cacher, continuez à utiliser l'e-mail comme vous l'avez toujours fait.

Autre problème à prendre en considération : l'identification du rédacteur des messages. Il existe en effet divers petits logiciels permettant d'envoyer des courriers en dissimulant ou en travestissant la véritable adresse de l'émetteur. Imaginez qu'un mauvais plaisant en utilise un et usurpe votre identité pour adresser des déclarations d'amour ou des lettres de menace à certaines de vos connaissances ou à des collègues de travail. Cela pourrait vous attirer de sérieux ennuis.

Heureusement, il existe diverses méthodes qui incluent dans tous vos messages une sorte de "signe électronique" qui vous authentifie automatiquement comme leur auteur, ou tout du moins qui atteste qu'ils ont bien été envoyés depuis votre ordinateur. A côté de cela, vous pouvez toujours avoir recours à la signature électronique, telle qu'elle est consacrée par la loi (*infra*, n^{os} 137 et s.).

Des problèmes liés à la sécurité peuvent également survenir. En effet, le courrier électronique peut également propager des virus informatiques (*infra*, n^{os} 108 et s.). Les virus se trouvent généralement dans les fichiers joints exécutables, mais peuvent aussi apparaître à l'intérieur d'autres types d'application (fichiers de traitement de texte, par exemple).

L'usage du courrier électronique soulève enfin la question de la preuve de l'existence et du contenu du message envoyé. Cette preuve se pose notamment dans le cadre du commerce électronique (*infra*, n° 133). Ce problème peut largement être résolu par le recours à une signature électronique sécurisée.

25. Comment puis-je m'assurer de la réception du courrier électronique par le destinataire ?

Lorsque vous envoyez un courrier électronique, plusieurs problèmes peuvent survenir.

Il se peut d'abord que, pour des raisons techniques, vos messages n'arrivent pas à destination. Le problème peut notamment provenir du serveur de votre correspondant ; celui-ci peut être inaccessible pour cause de panne. Dans ce cas, votre message vous est en principe renvoyé rapidement.

Le problème peut aussi être dû à une distraction de votre part ; vous pouvez avoir mal orthographié les coordonnées électroniques du destinataire du message. Dans ce cas le serveur renvoie le message et l'accompagne d'un message à son expéditeur, en indiquant son incapacité à acheminer le message (*User* ou *Host unknown*).

Même en l'absence de problème technique, vous pouvez vous demander toutefois si votre correspondant a bien reçu le message que vous lui avez envoyé. S'il ne répond pas, c'est peut-être que le serveur de votre correspondant l'a reçu, mais que votre correspondant n'a pas relevé son courrier.

Pour éviter le désagrément que peut causer une telle incertitude, vous pouvez activer dans votre logiciel la fonction "accusé de réception". Toutefois, en l'absence de tiers attestant l'envoi et, vu les innombrables possibilités de "trafiquer" la date et l'heure, la valeur de cet accusé est aléatoire. En outre, le destinataire est généralement avisé de la demande d'accusé de réception et doit en accepter l'envoi. Inutile de dire qu'il s'empressera de le refuser si le message lui est défavorable.

Pour ces raisons, le législateur a libéralisé le recommandé électronique, en ne laissant subsister le monopole de La Poste que pour les envois papiers (*infra*, n° 143). A l'instar de l'envoi recommandé traditionnel, il permet à l'expéditeur d'un message signé électroniquement de se constituer une preuve de son envoi, de sa date et, le cas échéant, de sa réception. Cette possibilité nécessite l'intervention d'un tiers de confiance, jouant en quelque sorte le même rôle que La Poste. Il atteste l'envoi grâce au récépissé électronique remis lors du dépôt ; il conserve la date et l'heure de l'envoi ; il peut enfin utiliser des outils techniques qui prouvent la réception.

26. Qu'est ce qu'un *hoax* ?

L'*hoax* est un message de fausse information, un canular. Les canulars (*hoax*) ne sont pas nés avec Internet, mais ils ont trouvé avec l'e-mail un vecteur de propagation privilégié.

Les *hoax* les plus courants concernent l'apparition d'un soi-disant virus extrêmement dangereux. Ils peuvent également prendre la forme de chaînes pyramidales : un message sollicitant par exemple votre solidarité envers une cause et qui vous invite à "passer ce message à vos connaissances".

L'*hoax* obéit souvent à la même structure. Le message ne vous est pas écrit personnellement mais est envoyé à une liste de correspondants, peu importe que vous connaissiez ou non l'expéditeur. Le contenu du message utilise les grands moyens pour attirer votre attention en vous intriguant ou en vous inquiétant (messages d'alerte, scénarios rocambolesques, etc.). L'information communiquée est cautionnée par des références dignes de foi. Enfin, on vous recommande, voire on vous ordonne, de faire passer le message à vos amis ou à tout votre carnet d'adresses.

Comme tel, un *hoax* ne peut représenter un danger pour votre ordinateur ; les risques de ces canulars résident ailleurs mais sont néanmoins réels. En effet, chacun croyant relayer une information importante ou voulant amuser la galerie transmet le message à une dizaine de personnes qui, à leur tour font de même ; la multiplication de ces messages a pour conséquence d'encombrer le réseau. Cela ralentit toutes les connexions, les transferts de données sont plus longs et donc plus chers.

A cette nuisance, s'ajoutent d'autres conséquences tout aussi néfastes, en fonction du thème de l'*hoax* : risque de propagation de vrais virus par ce type de courrier, incitation à effacer des fichiers sains sous prétexte de virus, escroquerie financière pour les chaînes pyramidales, détournement de signatures à partir de fausses pétitions, jusqu'à la diffamation et l'atteinte à l'image lorsque des personnes et des sociétés sont nominativement mises en cause.

Pour lutter contre ce type de pratique, il vous est conseillé de ne surtout pas diffuser de tels messages sans en avoir vérifié la source. Pour identifier la valeur d'un message et pour vous aider à reconnaître les différents types de canulars, vous pouvez consulter le site http://www.hoaxbuster.com. Enfin, il est également opportun que vous envoyiez un message courtois à votre expéditeur afin de lui signaler ce genre de pratiques néfastes.

Section 2. Le "chat"

27. Qu'est-ce que le "*chat*" ?

Le *chat*, que l'on peut traduire en français par "bavardage", désigne l'*Internet Relay Chat* (IRC).

Ce système vous permet de dialoguer par écrit et en temps réel via Internet avec toute personne pratiquant l'IRC au même moment, n'importe où dans le monde (pour peu qu'elle ait choisi le même réseau IRC). On peut alors avoir des conversations très vivantes avec un ensemble de correspondants sur un thème donné, dans des salles de conversations virtuelles appelées *chat rooms*. Sur l'IRC, chaque internaute est identifié par un mot de son choix, un pseudonyme.

Techniquement, l'IRC se présente comme une immense toile d'araignée composée de multiples serveurs. Certains serveurs sont reliés entre eux : ils forment ce que l'on appelle un réseau IRC. Toutes les personnes connectées à un même serveur peuvent donc dialoguer entre elles en direct ou avec celles connectées à un autre réseau.

28. Comment puis-je accéder au "*chat*" ?

Pour pratiquer le *chat*, il vous est nécessaire de vous connecter à un serveur IRC, de choisir un réseau IRC et d'établir la liaison avec le serveur IRC

L'accès au *chat* nécessite également l'installation d'un logiciel adéquat. Ce logiciel vous permet de vous connecter à un serveur IRC. Une fois connecté à un serveur, il vous reste à choisir un canal (*channel*) auprès de ce serveur, c'est-à-dire une pièce imaginaire dans laquelle se déroulera la discussion. Chaque canal de discussion traite d'un thème particulier et toute personne qui y est connectée reçoit tous les messages qui y sont adressés et peut intervenir.

Pour intervenir, il faut savoir que le *chat* possède son propre langage (voir notamment l'usage des *smileys*). Les discussions ayant lieu en temps réel, il faut écrire le plus rapidement possible. C'est pour cette raison que de nombreux raccourcis ont été créés.

Chaque canal possède son mode de fonctionnement : connectez-vous et observez avant d'intervenir.

29. Quels sont les risques liés au "*chat*" ?

Pratiquer l'IRC revient à entrer dans un bar et bavarder avec le premier venu. Dès lors, n'attendez pas trop de choses du *chat* ; ainsi vous ne serez pas déçu. Des interventions d'inconnus peuvent venir parasiter une conversation en cours. Un autre risque est de voir un internaute profiter de la situation (anonymat relatif, distance) pour devenir grossier envers ses correspondants.

Pour contrôler les dérives que pourrait encourager l'anonymat, une hiérarchie existe sur les canaux. Le fondateur du canal, qui en définit le thème, acquiert d'office le statut

d'opérateur. Il peut décider d'exclure temporairement ou définitivement les internautes ne respectant pas les conventions du canal.

Chaque internaute peut aussi utiliser une "*ignore list*" afin de ne pas afficher les messages privés qui lui sont adressés.

Enfin, les risques existent surtout à l'égard des mineurs. Incitez-les à vous "présenter" leurs amis du *net*, à ne jamais donner d'informations très personnelles et surtout découragez-les de rencontrer en personne un prétendu ami internaute.

Section 3. Les forums de discussion

30. Qu'est-ce qu'un forum de discussion ?

Les forums sont des lieux virtuels dédiés aux discussions et aux débats (*newsgroup*). Contrairement aux dispositifs de dialogue en direct (*chat*), les échanges dans un forum s'effectuent en différé, c'est-à-dire qu'un message posté n'apparaît pas instantanément.

Il existe aujourd'hui des milliers de forums de discussion ; il en existe en effet sur pratiquement tous les sujets imaginables. Toutefois, si votre sujet de prédilection n'est pas encore recensé, vos pouvez toujours créer vous-même un forum de discussion. Il vous faudra cependant obtenir préalablement l'assentiment du serveur auprès duquel s'échangeront les "*news*".

31. Comment puis-je accéder à un forum de discussion ?

Les forums de discussion – sortes de salles de réunions thématiques virtuelles – sont structurés selon différentes langues ou organisations. On parle de "hiérarchies" pour séparer ces ensembles.

Chaque hiérarchie est organisée en forums thématiques. L'usage veut que le nom de chaque forum soit formé de mots séparés de points, tout comme ceux des noms de domaines sur Internet. Le premier mot est commun à toute la hiérarchie (c'est d'ailleurs le plus souvent le nom donné à la hiérarchie : on parle de hiérarchie "be" pour l'ensemble des forums dont le nom commence par "be"), le second spécifie le cadre général des discussions dans ce forum (social, informatique, artistique ou autre), les mots suivants définissent plus ou moins précisément, selon leur ordre d'apparition, le thème particulier du forum.

Un forum dont le nom serait, par exemple, "be.rec.sport.petanque" ferait partie de la hiérarchie "be" (et serait donc régi par les règles d'usage générales définies pour cette hiérarchie), dans le domaine récréatif, et traiterait d'un sport, et plus spécifiquement de la pétanque.

Dans chacun de ces forums se déroulent donc des conversations dont le thème dépend du titre et de la description du forum. Il peut y avoir un grand nombre de discussions séparées les unes des autres à l'intérieur d'un seul et même forum, chacune étant distincte des autres grâce aux titres des articles postés dans cette discussion, et grâce aux références techniques qui sont présentes dans les champs techniques prévus à cet effet dans chaque article.

Au niveau du forum, tout utilisateur est soit un lecteur passif, qui se contente de suivre les débats, soit un utilisateur actif, qui poste des articles. Ce sont ces articles qui constituent le

contenu du forum et qui, lorsqu'ils participent d'une seule conversation, sont regroupés sous forme de [thread/fil/enfilade].

Un article posté dans un forum peut être lu par n'importe qui, à n'importe quel moment sur le serveur tant que la date d'expiration de l'article n'est pas dépassée. Cette "date d'expiration" varie selon les serveurs qui stockent les articles du forum, mais certains systèmes permettent de lire des articles postés depuis plus de 2 ans.

32. Quels sont les risques liés à l'utilisation d'un forum de discussion ?

Le risque principal des forums de discussion est lié à leur nature. En effet, il ne faut pas perdre de vue qu'un forum de discussion est un espace ouvert, public et, d'une certaine manière, non protégé. Le nombre de personnes pouvant avoir accès au forum de discussion auquel vous participez est illimité. Concrètement, au vu de cette diversité, cela signifie que les forums de discussion laissent la porte ouverte au meilleur comme au pire en termes de contenu de l'information.

Dans ce contexte, que vous soyez un utilisateur actif ou passif, vous devez être conscient que les propos tenus à l'occasion d'un forum de discussion peuvent être constitutifs d'infractions pénales telles que la diffamation, le racisme et la xénophobie, le révisionnisme, etc. En effet, celui qui s'exprime sur un forum de discussion doit prendre autant de précautions que celui qui s'exprime dans la presse écrite ou audiovisuelle. En conséquence, il faut veiller, le cas échéant, à modérer certains de vos propos ou ne pas hésiter à dénoncer ceux qui vous semblent de nature abusive, particulièrement en ce qui concerne les mineurs ou lorsque ces messages leur sont adressés.

Toutefois, quelques *newsgroups* sont "modérés". Cela signifie que tous les messages adressés au groupe de discussion transitent par une personne, un modérateur, dont la fonction consiste à contrôler le contenu des messages et des fichiers avant de les diffuser. L'objectif d'une telle démarche est de vérifier que les messages postés sont en rapport avec le sujet du forum et conformes à l'éventuelle "charte" qui le régit. Il ne s'agit cependant pas pour le modérateur de vérifier l'exactitude des informations reçues. Que les *newsgroups* soient ou non modérés, il n'existe aucune garantie quant à la qualité des informations diffusées.

Enfin, les forums de discussion sont une source d'informations particulièrement tentante et sans précédent pour les prospecteurs. De fait, les *newsgroups* permettent souvent d'identifier les adresses e-mails des internautes qui y adhèrent. Il est ainsi possible de dresser un profil commercial très ciblé, en fonction des listes thématiques sur lesquelles ils se sont inscrits. Il existe également des risques de collecte "sauvage" de vos données à caractère personnel (*infra*, n^{os} 81 et 82), bien que cette pratique soit totalement prohibée (*infra*, n° 74).

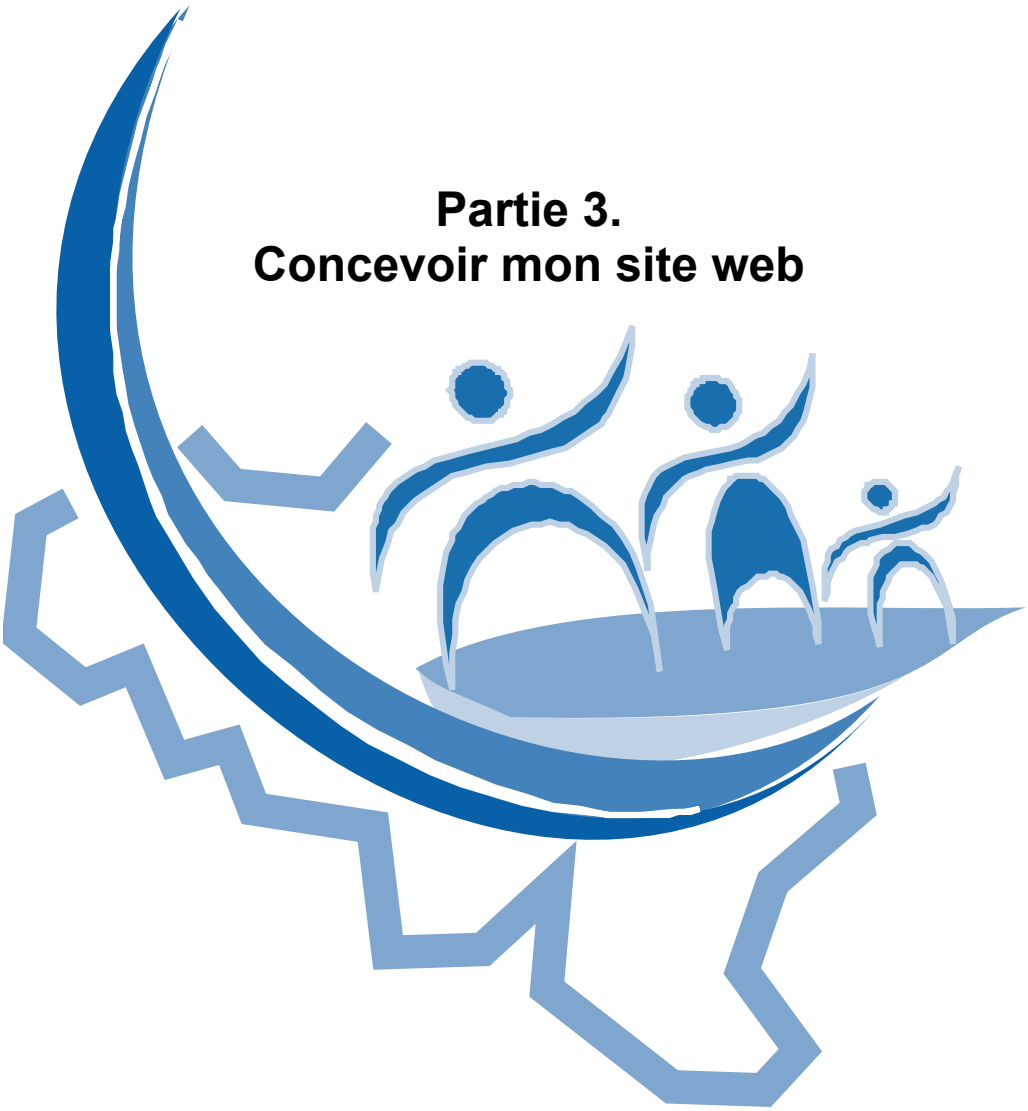
33. Qu'est-ce que la Nétiquette ?

La Nétiquette est le nom donné au code de conduite que l'on vous invite à respecter si vous utilisez Internet, principalement pour communiquer avec d'autres utilisateurs. Il s'agit en fait d'un ensemble de règles de civilité et de protocole à respecter si vous ne voulez pas vous fâcher avec vos interlocuteurs.

Si vous transgressez les règles en vigueur ou si l'on juge vos propos inappropriés, vous vous exposez à une réprimande (*flame*) de la part d'un autre utilisateur. Parmi les sujets les plus susceptibles de déclencher une véritable "guerre des *flames*" (série de messages provoqués par l'irritation mutuelle des différents utilisateurs), citons : la politique, la religion,

le sexe, sans oublier tout ce qui touche de près ou de loin à l'informatique (systèmes d'exploitation, langages de programmation, ordinateurs, etc.).

Partie 3.
Concevoir mon site web



Dans le but de vous faire connaître ou de partager l'un ou l'autre de vos centres d'intérêts par exemple, il vous est loisible de créer votre site web personnalisé. A cet effet, il existe de nombreux logiciels qui permettent d'éditer aisément des pages en HTML. Par ailleurs, les fournisseurs d'accès (gratuits ou payants) proposent généralement un espace mémoire (de plusieurs Mbytes) sur leur serveur afin de stocker votre page web et de la rendre disponible sur Internet.

Vous êtes en principe libre, lors de la création de votre site web, de déterminer sa présentation et son contenu : place est faite à votre imagination et à votre créativité. Est-ce à dire que vous pouvez y inclure tout et n'importe quoi ? Assurément, non !

Vous êtes avant tout tenu de respecter les droits d'autrui (droit d'auteur, droit à l'image, droit des marques, droit au respect de la vie privée, etc.) et le contenu ne peut être illégal ou avoir un caractère préjudiciable (propos racistes ou révisionnistes, diffamatoires, attentatoires à l'image, etc.). Vous devez également être prudent lorsque vous diffusez des informations (votre responsabilité pourrait être mise en cause !) et songer au respect de votre vie privée et de celle des autres lors de l'introduction de données à caractère personnel.

A l'inverse, il se peut que vous ayez créé une page web véritablement originale. A ce titre, elle fera l'objet d'une protection juridique.

Mais avant d'aborder ces différentes questions, vous devrez nécessairement réfléchir à un endroit pour stocker votre page web et surtout à une adresse afin que tout internaute puisse la retrouver sur Internet. C'est la question du nom de domaine.

CHAPITRE I. LA RESERVATION D'UN NOM DE DOMAINE

34. Qu'est-ce qu'un nom de domaine ?

Afin de pouvoir assurer le fonctionnement correct d'Internet, chacun des millions d'ordinateurs interconnectés est identifié par une adresse IP (*Internet Protocol*) qui prend la forme de 4 nombres contenant chacun au maximum 3 chiffres compris entre 0 et 255. Par exemple, l'adresse IP du site de la Chambre est 212.35.105.232., celle de la Commission de la Protection de la Vie Privée est 212.190.77.114. ou encore celle du Service public fédéral Economie, PME, Classes moyennes et Energie est 193.191.210.45. Pour avoir accès au site de ces institutions, il vous suffit d'introduire cette adresse à l'endroit prévu par votre logiciel de navigation, comme vous le montre l'image ci-dessous.

Toutefois, si les ordinateurs s'accommodent bien de la lecture et de la compréhension de cette suite de chiffres, on se rend compte que pour l'internaute, l'utilisation de ces caractères numériques n'a rien de commode. Afin de faciliter la mémorisation et de rendre les adresses plus conviviales, ces nombres (adresses IP) peuvent être convertis en un nom de domaine compréhensible pour l'utilisateur C'est d'ailleurs ce qui se fait communément sur le *net* où vous ne tapez pas 212.35.105.232., mais plus simplement "http://www.lachambre.be" qui est automatiquement traduit – de façon transparente pour l'utilisateur – en une adresse IP correspondante. Cette conversion est assurée par un système de conversion appelé DNS (*Domain Name System*), constamment remis à jour.

Ainsi, vous pourriez demander pour votre société *(http://www.alabonnefrite.be ou .com)* ou pour vous-même *(http://ww.dupont.be ou .org)* un nom de domaine sous la forme d'une adresse qui vous identifie clairement et qui permet aux internautes d'accéder facilement à votre page web.

35. Dois-je obligatoirement acquérir un nom de domaine ?

NON. Vous n'êtes pas obligé d'acquérir un nom de domaine pour localiser votre page web. L'avantage de posséder un nom de domaine est que l'adresse est réellement personnalisée. Le désavantage est que cela se paye ! L'enregistrement d'un nom de domaine donne lieu à la facturation d'une redevance annuelle par l'agent DNS que vous avez choisi. Dans la majorité des cas, l'enregistrement d'un nom de domaine n'est pas le seul service que vous recevrez de votre agent DNS. L'enregistrement sera souvent accompagné par des services complémentaires, tels que le *hosting* du site, l'*e-mail* et l'*URL-forwarding*. Le prix d'enregistrement du nom de domaine ne constitue donc le plus souvent qu'une petite partie du prix complet pour l'ensemble de ces services.

Si vous ne possédez pas de nom de domaine, vous pouvez néanmoins disposer d'un espace disque sur le serveur de votre *provider* (fournisseur d'accès Internet). Ce service est généralement gratuit ou inclus dans votre abonnement payant d'accès à Internet. Dans ce cas, votre page sera localisée en fonction du nom du *directory* (répertoire) créé pour stocker votre page web sur ce serveur. L'adresse pour localiser cette page sera donc composée de deux parties : d'une part, le nom de domaine de votre *provider* et d'autre part, le nom de votre *directory* (par exemple http://users.provider.be/dupont). Cette solution ne vous coûtera en principe rien mais ne permet pas de posséder une adresse véritablement personnalisée et donc limite votre visibilité sur Internet. Par ailleurs, cette adresse manque de souplesse en ce sens que vous ne pouvez pas la réutiliser si vous changez de fournisseur d'accès.

36. Comment se compose un nom de domaine ?

Si vous optez pour l'obtention d'un nom de domaine, deux étapes sont nécessaires pour déterminer celui-ci : choisir le radical et l'extension. Ceci doit être fait soigneusement sachant que la visibilité du site sur Internet en dépend. En général, le *radical* correspond au nom de la personne physique ou morale qui gère le site, et l'*extension* au type d'activité exercée ou à la zone géographique où sont exercées ces activités. Les sociétés commerciales enregistreront plutôt en ".com", ".biz" ou en ".be", les particuliers en ".be", ".name" ou en ".info", les organisations et associations sans but lucratif en ".org" ou ".net", les organismes internationaux en ".int", etc.

37. Quelles sont les extensions existantes ?

Deux types d'extensions existent aujourd'hui sur Internet.

Le premier englobe les extensions dites *"territoriales*" qui, comme le nom l'indique, dépendent de leur rattachement géographique. Elles sont composées de deux lettres identifiant le pays d'origine du site. Elles sont particulièrement nombreuses et vont de ".ac" pour Ascension Islands à ".zw" pour le Zimbabwe, en passant par ".be" pour la Belgique. Certains organismes gérant l'attribution des noms de domaine "nationaux" prévoient des règles pour l'enregistrement de leur extension, *mais d'autres comme ".tv" (Tuvalu), ".md" (Moldavie), ".ac" (Iles Ascensions) et ".vg" (Iles Vierges) ne prévoient pas de conditions strictes pour l'enregistrement, ou même ne prévoient aucune condition. Ces dernières extensions ne sont donc plus vraiment territoriales.* Elles se rapprochent plutôt des

extensions génériques comme le ".com" en ce sens que n'importe quel utilisateur, même s'il ne réside pas sur le territoire en question, peut en faire la demande.

Dans le cadre des extensions territoriales, une nouvelle extension particulière devrait voir le jour prochainement : il s'agit du ".eu". En effet, le Conseil de l'Union européenne et le Parlement européen se sont mis d'accord dernièrement pour mettre en œuvre celle-ci, estimant que c'est une des priorités de l'initiative e-Europe. Le ".eu" sera réservé aux organisations, entreprises et personnes physiques établies sur le territoire de l'Union européenne. L'objectif essentiel de cette nouvelle extension est de permettre l'identification d'acteurs opérant sous un régime juridique harmonisé en matière de commerce électronique et offrant notamment un niveau élevé de protection au consommateur. En principe, le ".eu" sera en principe disponible en 2003.

Le second type vise les extensions liées au type d'activité. Celles-ci contiennent trois lettres ou plus identifiant la sphère d'activité de l'utilisateur. Cela recouvre les extensions génériques ".com" pour les sociétés commerciales, ".net" pour les sites liés au fonctionnement d'Internet et ".org" pour les organisations et organismes non lucratifs ainsi que les extensions réservées à des organismes spécifiques : ".gov" pour les organisations gouvernementales, ".int" pour les institutions internationales, ".mil" pour les activités militaires et ".edu" pour le monde de l'éducation. Plus récemment, de nouvelles extensions ont fait leur apparition telles que ".biz" pour les entreprises, ".info" pour les entreprises et particuliers, ".name" pour les particuliers et ".coop" pour les coopératives. Les extensions "pro", "museum", "aero" ont été également approuvées et elles sont opérationnelles.

Il ne vous est pas interdit d'enregistrer divers noms de domaines ayant le même radical, mais reprenant des extensions différentes. Selon l'extension que vous choisirez, il vous faudra simplement contacter l'autorité responsable de l'attribution du type de nom de domaine choisi, respecter les éventuelles contraintes qu'elle vous imposera et payer la redevance appropriée, sans oublier de vérifier au préalable que le nom de domaine n'est pas déjà enregistré.

38. A qui dois-je m'adresser pour enregistrer un nom de domaine ?

D'un point de vue pratique, le plus simple est de vous adresser à votre fournisseur d'accès qui effectuera, moyennant paiement, les démarches pour vous en vue d'enregistrer le nom de domaine demandé en ".be" mais aussi dans d'autres extensions. Dans certains cas, vous pouvez directement vous adresser à l'organisme responsable pour l'une ou l'autre extension (vous trouverez les organismes responsables pour chaque extension à l'adresse suivante : http://www.iana.org/domain-names.htm). Sachez toutefois que, pour le ".be", il n'est plus possible de passer par l'ASBL DNS.BE pour procéder à l'enregistrement d'un nom de domaine avec cette extension. Il y a lieu, en effet, de passer par l'intermédiaire d'un agent agréé par cette ASBL. Vous trouverez sur le site http://www.dns.be la liste des agents agréés par le DNS.BE, ainsi que la procédure à suivre pour enregistrer un nom de domaine en ".be".

39. Faut-il remplir des conditions pour obtenir un nom de domaine ?

En ".com", ".org" et ".net" il n'y a aucun critère spécifique à remplir si ce n'est la disponibilité du nom de domaine. En Belgique, le ".be" était jusqu'en décembre 2000 réservé aux sociétés commerciales, aux organisations ou institutions publiques ou privées et aux associations ayant une activité légale "réelle et raisonnable". Par ailleurs, ces sociétés ou organisations devaient être situées ou représentées en Belgique. Depuis cette date, le DNS.BE a revu complètement ses règles de fonctionnement, notamment pour avoir

constaté que les règles strictes appliquées en vue d'éviter les enregistrements abusifs avaient eu pour effet de détourner une partie des sites belges vers des domaines génériques (".com" par exemple) dont l'attribution est moins contraignante.

Désormais, l'extension ".be" est ouverte à tous : tant aux entreprises qu'aux particuliers belges ou étrangers, qui ne doivent plus répondre à des conditions spécifiques pour enregistrer un nom de domaine. Par ailleurs, l'enregistrement des noms génériques est autorisé, sauf indication contraire du DNS.BE. Une fois enregistré, vous obtenez une licence d'utilisation pendant une période d'un an. N'oubliez donc pas de payer votre redevance annuelle pour le renouvellement de la licence, au risque de perdre votre droit d'utiliser le nom de domaine ! Par ailleurs, l'enregistrement est soumis à l'acceptation de conditions générales (disponibles sur le site http://www.dns.be) que nous vous conseillons de lire préalablement.

40. Puis-je obtenir n'importe quel nom de domaine ?

NON ! Même si la plupart des gens pensent que tout nom de domaine qui n'a pas encore été réservé peut être librement enregistré – c'est le principe du "premier arrivé, premier servi" -, il est nécessaire d'apporter de sérieuses nuances à ce principe. En effet, tout d'abord, il convient de respecter le ou les droits que les tiers peuvent détenir sur un nom de domaine (marque, nom commercial, nom patronymique, etc.), spécialement si vous ne disposez d'aucun droit sur le même nom de domaine. Ensuite, les juges sont de plus en plus attentifs à punir ceux qui réservent en masse des noms de domaine de sociétés connues dans le seul but de les revendre à prix d'or. Certes, votre enregistrement du nom de domaine ne sera pas refusé puisque les différentes sociétés qui sont autorisées à enregistrer les noms de domaines effectuent leur tâche sans contrôler *a priori* le respect du droit que d'autres personnes pourraient avoir sur le nom que vous voulez enregistrer. Mais si un tiers porte plainte et que le juge ou un arbitre reconnaît des droits légitimes dans son chef, on pourra vous forcer à céder ce nom de domaine au tiers revendiquant.

Ainsi, rien ne semble donc vous interdire d'enregistrer "*alabonnefrite.com*" si cette société ne l'a pas encore fait. Pourtant, il peut arriver que le nom de domaine que vous avez choisi soit tôt ou tard contesté par la société Alabonnefrite dont vous avez utilisé la marque ou simplement le nom commercial. Il pourrait en être de même si vous enregistrez le nom de domaine "*celinedion.be*", alors qu'aucun membre de votre famille ne porte ce nom, pas plus que vous-même. Sachez que, si vous avez fait du *domain name grabbing*[1] ou *usurpation de nom de domaine,* le juge pourrait vous condamner à céder le nom de domaine litigieux au titulaire des droits sur celui-ci (la société Alabonnefrite ou Céline Dion) et vous condamner éventuellement à des dommages et intérêts.

Afin d'éviter tout problème, *nous vous conseillons* donc de choisir votre nom de domaine en toute bonne foi, sans intention de nuire, ni but lucratif et pour une raison valable (vous aimez l'horticulture, vous avez enregistré "fleurs.com" pour y faire figurer un site sur les fleurs d'Afrique). Dans ce cas, votre nom de domaine ne devrait, en principe, pas vous être contesté. Veillez également à ne pas réserver un nom de domaine contenant le nom d'une marque renommée, car ces marques sont particulièrement protégées et il vous sera difficile de prouver que vous avez une raison valable d'utiliser ce nom de domaine (un juge

[1] Pratique qui consiste en l'enregistrement intentionnel d'un nom de domaine contenant un signe utilisé par une tierce personne comme marque, nom commercial, nom patronymique, dans le seul but d'empêcher le propriétaire de cette marque d'enregistrer ce nom de domaine ou de lui revendre ce nom au prix fort.

acceptera sans doute difficilement que vous ayez réservé “dhl.com”, sous prétexte que vous avez assemblé les premières lettres de vos trois chiens Dumbo, Happy et Loulou et créé un site parlant de la race canine).

41. A qui puis-je m’adresser si je conteste la réservation par un tiers d’un nom de domaine ?

Bien entendu, si vous pouvez vous prévaloir de droits sur un nom de domaine déjà réservé “abusivement” par un tiers, il vous est loisible de porter le litige devant les tribunaux compétents. Le cas échant, le juge pourrait condamner le tiers à vous transférer le nom de domaine litigieux ainsi qu’à vous payer d’éventuels dommages et intérêts. Toutefois, cette procédure peut s’avérer longue et coûteuse.

Vu ces inconvénients, le DNS.BE a mis en place une procédure “alternative” de règlement des litiges efficace, rapide (quelques semaines) et peu onéreuse (1.600,00 EUR pour récupérer de 1 à 5 noms de domaine). Celle-ci consiste à soumettre les litiges concernant un nom en “.be” au CEPANI (Centre Belge d’Arbitrage et de Médiation : www.cepani.be). Ce centre a élaboré expressément un règlement pour la résolution des litiges concernant des noms de domaine (disponible à l’adresse : http://www.cepani.be/noms_de_domaine_reglement.html). Les parties qui le souhaitent peuvent donc soumettre leur litige à un “tiers décideur” qui se trouve sur la liste publiée par le CEPANI. La décision de ce tiers indépendant se limite soit à un rejet de la demande, soit à une radiation du nom de domaine et au transfert de l’enregistrement de celui-ci au bénéfice du requérant. Par contre, cette procédure alternative ne permet pas d’obtenir réparation – consistant en l’octroi de dommages et intérêts – d’un préjudice éventuellement subi. Par ailleurs, vous pouvez à tout moment saisir les tribunaux traditionnels dont la décision l’emporte sur celle du tiers décideur.

Si une procédure judiciaire ou arbitrale est introduite contre l’utilisation d’un nom de domaine, le DNS.BE met ce dernier en “*on hold*” jusqu’au prononcé de la décision finale concernant le litige. Pour le reste, le DNS.BE n’intervient pas dans l’administration ou le déroulement de la procédure de règlement du différend.

CHAPITRE II. QUE PUIS-JE METTRE SUR MON SITE SANS VIOLER LE DROIT DES TIERS ?

Lorsque vous créez votre page web, vous êtes tenu de respecter les droits d'autrui et notamment le droit qu'un auteur peut avoir sur une œuvre quelconque (texte, image, photo, séquence musicale ou vidéo, etc.) qu'il a réalisée.

Avant d'aborder les questions concrètes que vous pourriez vous poser, il paraît important de faire un rappel rapide des *principes essentiels du droit d'auteur*. Les législations concernées sont les suivantes : principalement, la loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins, mais aussi la loi du 30 juin 1994 relative à la protection des programmes d'ordinateur, ainsi que la loi du 31 août 1998 concernant la protection juridique des bases de données.

Sur Internet, le droit d'auteur n'est pas toujours respecté ! En effet, les possibilités offertes par les nouvelles technologies (la redoutable fonction *copier/coller*, le fait qu'il suffit d'appuyer sur un bouton pour imprimer un document de plusieurs centaines de pages, la possibilité de scanner rapidement des œuvres, l'utilisation des moteurs de recherche qui permettent de trouver très rapidement l'image ou la photo que l'on cherche, etc.) sont telles qu'il est encore plus facile d'exploiter l'œuvre d'autrui que cela ne l'est dans l'environnement traditionnel. Ainsi, la quantité d'actes (reproduction, modification, etc.) contraires aux droits d'auteur et la rareté de réaction des auteurs victimes de ces actes sont telles qu'on pourrait croire que ces droits n'existent pas (ou plus) et que tout est permis sans risque aucun !

Et pourtant, c'est faux. Tout n'est pas permis, même sur Internet. Plusieurs décisions de jurisprudence, qui ne sont que les premières d'une longue série, montrent que le droit d'auteur est toujours d'application et que son non respect peut être lourdement sanctionné.

Section 1. Principes essentiels du droit d'auteur

Le droit d'auteur confère aux auteurs des droits exclusifs relatifs à l'utilisation de leur œuvre. Il en résulte qu'il faut généralement, pour utiliser une telle œuvre (pour une reproduction telle qu'une photocopie, une impression, un *copier/coller*, pour une modification ou pour une communication au public, ce qui est le cas lorsqu'on met un site web en ligne), obtenir l'autorisation préalable du titulaire de droits sur l'œuvre.

Sur Internet, ces utilisations sont fréquentes. Par exemple, le tenancier du cyber-café de Besançon qui a diffusé l'ouvrage "Le grand secret" du Docteur Gubler sur Internet avait préalablement scanné le livre (première reproduction), le fichier avait ensuite été mis sur sa page web et donc sur un serveur (seconde reproduction et "communication au public" de l'oeuvre), les personnes qui visitaient le site pouvaient alors télécharger le texte (autre reproduction) et éventuellement le réimprimer sur papier (dernière reproduction). D'autre part, on peut également considérer qu'il y a eu communication au public, ce qui relève du droit exclusif de l'auteur, par le seul fait de rendre l'ouvrage accessible, via le site web, à un large public.

Par respect des principes du droit d'auteur, il est clair que ce tenancier aurait dû obtenir préalablement l'autorisation du titulaire des droits. Il en est de même pour les étudiants français qui avaient numérisé et mis en ligne les paroles de chansons de Brel et de Sardou et qui ont été condamnés pour cette raison. On peut en conclure qu'avant de diffuser une œuvre sur Internet, il faut avoir obtenu l'autorisation du titulaire des droits (qui est souvent mais pas toujours le créateur de l'œuvre car il peut avoir cédé ses droits, en particulier à une société de gestion collective des droits d'auteur).

42. Quels sont les éléments protégés par le droit d'auteur ?

Est protégée par le droit d'auteur toute œuvre originale et coulée dans une certaine forme. Que signifient ces concepts d'œuvre, d'originalité et de forme?

La notion *d'œuvre* est interprétée d'une manière très large. Elle vise notamment :

- les **textes** de toute nature (romans, nouvelles, poèmes, textes scientifiques ou techniques, etc.) et cela, indépendamment de leur contenu, de leur longueur, de leur destination (divertissement, éducation, information, publicité, propagande, etc.), de leur forme (manuscrite, dactylographiée, imprimée ou sous forme électronique) ;

- les **photographies**, indépendamment de leur support (papier ou numérique) et de leur objet (personne, paysage, événements d'actualité, tableau dans le domaine public, etc.) ;

- les **images**, qu'elles soient virtuelles ou non, et peu importe leur type (dessins, sigles, icônes, logos, cartes géographiques, etc.) ;

- les **séquences musicales, vidéos ou audiovisuelles** en général, quel que soit le format ou le support d'enregistrement ;

- les **programmes d'ordinateur** (des logiciels de jeu).

Pour qu'elle soit protégée, l'œuvre doit être *originale*. Il s'agit d'un critère abstrait, difficile à définir en pratique, qui signifie que l'œuvre doit porter l'empreinte de la personnalité de son auteur. On ne rentrera pas dans les détails de ce concept, mais il faut savoir que le caractère original d'une œuvre est une question de fait souverainement appréciée par le juge. Il n'est donc pas possible de savoir si une œuvre est considérée comme originale ou non tant que le juge ne s'est pas prononcé sur ce caractère. Néanmoins, il convient de noter que la jurisprudence apprécie cette notion d'originalité d'une manière très souple. Il en résulte qu'une œuvre sera considérée dans la plupart des cas comme originale. Attention : original ne veut en aucun cas dire beau ! L'originalité est une notion qui ignore l'esthétique. Ce n'est donc pas parce que vous trouvez une œuvre laide, voire ridicule, que celle-ci ne pourra pas être jugée originale.

Pour qu'une œuvre bénéficie de la protection, il faut en outre qu'elle soit matérialisée dans une *forme* particulière susceptible d'être appréhendée par les sens. Cette condition ne pose pas de problèmes pour le cas des œuvres accessibles en ligne puisqu'elles ont nécessairement dû faire l'objet d'une mise en forme préalable pour être rendues visibles. Cette condition signifie qu'*a contrario*, le droit d'auteur ne protège ni les idées (même si elles sont *géniales* ou *originales*), ni les méthodes ou les styles, même originaux (on peut donc, lors de la création d'un site web, s'inspirer des styles utilisés par d'autres, à la condition que l'on ne copie aucun élément formel original).

43. Existe-t-il d'autres conditions pour bénéficier de la protection par le droit d'auteur ?

NON, il n'existe aucune autre condition pour bénéficier de la protection par le droit d'auteur. Il faut et il suffit que l'œuvre soit originale et mise en forme.

Il n'est donc pas nécessaire d'accomplir des formalités telles que le dépôt d'un exemplaire de l'œuvre auprès d'une administration ou l'indication de la mention *copyright* © (il est toutefois conseillé d'effectuer ces formalités pour des raisons probatoires). La protection naît par le seul fait de la création de l'œuvre.

Par contre, si vous souhaitez bénéficier de la protection d'un signe distinctif par le droit des marques (qui doit être distingué du droit d'auteur), il est dans ce cas nécessaire de procéder à un dépôt de la marque en bonne et due forme.

44. Quels sont les droits de l'auteur sur son œuvre ?

Autrement dit, quels droits devez-vous obtenir si vous désirez utiliser l'œuvre d'autrui dans le cadre du développement de votre site web ?

L'auteur dispose en réalité de deux types de droits :

- des *droits patrimoniaux* (droits qui permettent à l'auteur de retirer un bénéfice économique de l'exploitation de son œuvre), qui sont cessibles et peuvent faire l'objet de contrats de licence ;

- des *droits moraux* (ils visent à protéger l'intégrité de l'œuvre, la relation de celle-ci avec son auteur et la réputation de ce dernier), qui sont incessibles (tout au plus peut-on y renoncer partiellement).

Les droits patrimoniaux

En résumé, les droits patrimoniaux sont les suivants :

- Le *droit de reproduction* au sens large :

Il s'agit d'une prérogative qui permet à l'auteur d'interdire ou d'autoriser que son œuvre soit reproduite et de définir les modalités de cette reproduction. Plus précisément, le droit de reproduction comprend :

- le *droit de reproduction au sens strict* : ce droit permet à l'auteur de déterminer le mode technique de reproduction (photographie, numérisation par scanner), le type de support (papier ou numérique), le lieu de la reproduction (sur un site web, sur un CD-Rom) et les conditions de la première mise dans le commerce des exemplaires. Ce droit recouvre la reproduction partielle ou non, temporaire ou définitive, directe ou indirecte ;

- le *droit d'autoriser l'adaptation et la traduction de l'œuvre* : ce droit vise la transposition de l'œuvre dans un genre différent (un texte adapté en texte interactif), les modifications de toute nature (le fait de résumer un texte, de *zoomer* ou changer les couleurs d'une photographie) et les traductions en toutes langues ;

- le *droit de location ou de prêt* : droit pour l'auteur de mettre l'original de son œuvre ou une reproduction de celle-ci à la disposition d'un tiers pour une durée

déterminée (le titulaire de ce droit pourrait, par exemple, interdire pendant plusieurs mois après leur sortie la location de CD-Rom afin de se donner le temps d'organiser la commercialisation de l'œuvre).

- Le *droit de distribution* :

Ce droit donne à l'auteur la possibilité de contrôler les modalités de la commercialisation de son œuvre (ce droit se rapproche du droit de reproduction au sens strict).

- Le *droit de représentation* ou *de communication au public* :

Ce droit vise la communication de l'œuvre au public, y compris sa mise à la disposition de manière telle que chaque membre du public puisse y avoir accès individuellement au moment et au lieu qu'il choisit. Ce droit couvre la transmission d'une œuvre *on-line* (sur Internet). Il s'agit ici de la communication directe au public, sans l'intermédiaire d'un support.

Les droits moraux

A côté des droits patrimoniaux, l'auteur dispose également de droits moraux qui constituent l'expression du lien existant entre l'auteur et sa création.

Les droits moraux sont les suivants :

- le *droit de divulgation* : ce droit permet à l'auteur de décider quand son œuvre est achevée et peut être présentée au public. Par conséquent, accéder à une œuvre inachevée (un morceau musical en cours de conception par exemple) et la mettre en ligne est une violation de ce droit, car l'auteur n'a pas encore donné son autorisation à la divulgation.

- le *droit de paternité* : ce droit signifie que l'auteur peut revendiquer la paternité de l'œuvre, c'est-à-dire décider que son nom (ou un pseudonyme) soit mentionné à l'occasion de l'exploitation de l'œuvre ou que celle-ci soit publiée de manière anonyme. S'approprier l'œuvre d'autrui est donc une violation de ce droit, tout comme le fait de la diffuser sous le nom de l'auteur si celui-ci ne le souhaite pas.

- le *droit à l'intégrité* : ce droit permet à l'auteur de s'opposer à toute modification de son œuvre (texte découpé ou résumé, photographie recadrée, modifiée par un filtre ou par des effets spéciaux) ainsi qu'à toute atteinte préjudiciable à l'honneur ou à la réputation (soit suite à une modification matérielle de l'œuvre, soit suite à une modification du contexte ou de la manière dont l'œuvre est présentée).

45. Pendant combien de temps l'œuvre est-elle protégée ?

La protection par le droit d'auteur est limitée dans le temps. La règle générale est que l'œuvre est protégée jusqu'à la fin d'une période de 70 ans après la mort de l'auteur. Il en résulte par exemple que les partitions de concertos composés par Mozart ne sont plus protégées par le droit d'auteur. Elles peuvent donc être reproduites (par exemple photocopiées) sans devoir obtenir l'autorisation des héritiers de Mozart (mais il faudra, le cas échéant, l'autorisation des musiciens interprètes et des maisons de disques).

46. Qu'est-ce qui n'est pas protégé par le droit d'auteur ?

N'est pas protégée par le droit d'auteur, et peut donc être reproduite, par exemple, sans l'accord de l'auteur :

- Une œuvre qui n'est pas originale ! Cette notion est fort relative et doit être appréciée par le juge. Il est donc déconseillé de prendre la liberté de décider si l'œuvre d'autrui est originale ou pas ;

- Une œuvre qui n'est plus protégée c'est-à-dire une œuvre dont l'auteur est décédé depuis plus de 70 ans (il faudra toutefois parfois obtenir l'accord d'autres titulaires de droits) ;

- Une œuvre visée par l'article 8 de la loi sur le droit d'auteur. Cet article prévoit que certaines œuvres, même originales, ne sont pas protégées par le droit d'auteur : ce sont les discours prononcés dans les assemblées délibérantes, dans les audiences publiques des tribunaux et dans les réunions politiques ainsi que les actes officiels de l'autorité (loi, décret, ordonnance, etc.).

La conséquence de cette non protection par le droit d'auteur est que ces œuvres peuvent notamment être librement reproduites et communiquées au public.

Rappelons qu'une idée, même originale, n'est pas protégée par le droit d'auteur tant qu'elle n'est pas mise en forme et donc concrétisée matériellement.

47. Ne puis-je jamais reproduire une œuvre protégée par le droit d'auteur ?

Il existe des hypothèses dans lesquelles il est possible de reproduire tout ou partie d'une œuvre protégée par le droit d'auteur, et ce, sans devoir obtenir l'autorisation de l'auteur. En effet, la loi sur le droit d'auteur contient quelques exceptions. On notera qu'elles sont limitées, soumises à des conditions strictes et qu'il n'est pas toujours aisé de s'en prévaloir dans le cadre de la conception et de la mise en ligne d'un site web. Il existe toutefois une exception pertinente dans le cadre de la conception d'un site web : le droit de citation.

Le droit de citation permet de reproduire un extrait d'une œuvre sans le consentement de l'auteur de celle-ci. Plusieurs conditions doivent toutefois être cumulativement remplies :

- la citation doit être extraite d'une œuvre "licitement publiée" (on ne peut donc pas citer une œuvre tant que son auteur n'a pas décidé de la divulguer au public) ;

- la citation doit être courte (il s'agit d'une question de fait à apprécier par le juge) ;

- la citation doit avoir lieu "dans un but de critique, de polémique, d'enseignement ou dans des travaux scientifiques" (cela exclut donc les citations dans le cadre d'un site web de divertissement ou purement commercial) ;

- la citation doit être faite de "bonne foi" ;

- la citation doit mentionner la source et le nom de l'auteur.

48. A qui dois-je m'adresser si je veux obtenir des autorisations ?

Il résulte des considérations qui précèdent que, pour exploiter une œuvre, il faut disposer du consentement de l'auteur, et donc contracter avec lui. Pour ce faire, vous devez vous poser trois questions :

- Qui est (quels sont) le(s) titulaire(s) des droits d'auteur sur l'œuvre ?
- L'auteur est-il toujours titulaire des droits ? Ne les a-t-il pas cédés ?
- L'auteur n'a-t-il pas confié la gestion de ses droits à une société de gestion des droits d'auteur ?

Principe

En principe, le titulaire du droit d'auteur est la personne physique qui a créé l'œuvre. Cette personne est le "titulaire originaire" des droits d'auteur. En vue de faciliter la charge de la preuve, la personne dont le nom (ou un signe quelconque) est mentionné sur l'œuvre est présumée titulaire des droits d'auteur.

Si l'œuvre a été créée par plusieurs personnes, il y aura en principe "œuvre de collaboration" et le droit d'auteur appartiendra à l'ensemble des créateurs de l'œuvre. Une personne ne pourra se prétendre coauteur de l'œuvre que si elle a effectivement apporté une prestation créative à la mise en forme de l'œuvre en cause (ce qui ne sera pas le cas de la personne qui ne fait que donner des idées ou qui ne fait qu'encoder des données techniques). Il y aura dès lors lieu de demander l'autorisation à chacun des coauteurs.

Il faut également être attentif au fait que, pour un site web ou une base de données, on peut envisager deux types d'auteur :

- l'auteur ou les coauteurs du site web : en effet, le site web sera souvent, en lui-même et indépendamment de son contenu, une œuvre protégée par le droit d'auteur en tant qu'agencement original des différents éléments ;
- l'auteur ou les auteurs, non plus du site web, mais des éléments incorporés dans ce dernier (une photographie, un logo, une séquence musicale).

La cession du droit d'auteur

Il se peut que l'auteur d'une œuvre ne soit plus titulaire des droits (patrimoniaux) parce qu'il les a cédés ou ne soit plus en mesure de concéder les droits car il a consenti une licence exclusive à un tiers. Ce dernier devient alors *titulaire dérivé* des droits d'auteur. Il faudra donc demander à l'auteur s'il est toujours titulaire des droits et, dans la négative, qui est le cessionnaire des droits. Par ailleurs, il conviendra éventuellement de respecter les droits moraux de ce même auteur, qui sont incessibles.

Les sociétés de gestion des droits d'auteur

L'auteur qui ne souhaite pas assumer seul la charge de la gestion de ses droits peut confier celle-ci à une société de gestion des droits d'auteur (SABAM, SOFAM, SESAM, SCAM). Cette solution présente notamment l'avantage pour l'utilisateur de n'avoir en face de lui qu'un seul interlocuteur pour la négociation des droits, ce qui n'est pas négligeable s'il veut exploiter de nombreuses œuvres.

Section 2. Les questions concrètes que vous vous posez !

49. Est-ce que je dispose des droits pour utiliser le logiciel d'édition de page web ?

Pour créer votre page web, vous allez probablement utiliser un logiciel d'édition approprié. Pour télécharger votre site web sur le serveur du fournisseur d'accès, vous allez également utiliser un logiciel *ad hoc*. Pour consulter votre site, vous allez utiliser un logiciel de navigation. Avez-vous le droit d'utiliser ces différents logiciels ? En d'autres mots, ceux-ci ne sont-ils pas par exemple des copies pirates ?

Cela peut paraître évident mais rappelons que les logiciels sont également protégés par le droit d'auteur. Ce n'est pas parce que vous avez acheté un logiciel sur un support que vous êtes titulaire des droits intellectuels sur ce logiciel. En pratique, il en résulte que l'utilisation d'un programme d'ordinateur implique l'autorisation du titulaire du droit d'auteur sur ce programme. Cette autorisation se concrétise par la conclusion d'une licence, qui est généralement concédée lorsque l'on achète le support CD-ROM ou la disquette contenant le programme.

50. Puis-je scanner une photo afin de l'inclure sur ma page web ?

En vue de rendre votre site web plus attractif, vous serez probablement tenté d'y insérer une ou plusieurs photos préalablement scannées (numérisées). Pouvez-vous scanner une photo analogique et l'insérer librement sur votre site? La solution n'est pas tranchée. Deux hypothèses doivent être distinguées.

1. Soit la photo a été prise par vous-même (photos de vacances, de votre famille, de votre collection de voitures, etc.) et vous êtes donc titulaire des droits d'auteur sur cette photo. Vous pouvez en principe la reproduire librement et la communiquer au public par le biais de votre site, *pour autant* que l'objet photographié ne soit pas lui-même protégé par le droit d'auteur (photographie d'une autre photographie protégée, d'une peinture, d'une sculpture ou d'un album de Tintin). Si c'est le cas, vous devez obtenir l'autorisation de l'auteur de l'objet photographié.

   Mais attention : les difficultés ne s'arrêtent pas là ! Si vous photographiez une personne, vous devez également respecter le droit à l'image de cette personne. Ce droit, qui n'est pas directement lié au droit d'auteur, permet à toute personne photographiée de s'opposer à toute reproduction (notamment sur Internet) et à toute communication au public (notamment via Internet) de son image. Vous devrez donc dans ce cas obtenir l'autorisation de la personne représentée. Sachez toutefois qu'il existe certaines exceptions pour les personnages publics ainsi que pour les personnes privées photographiées parmi la foule.

2. Soit vous scannez (numérisez) une photo que vous trouvez dans un livre ou un magazine dans le but de l'insérer sur votre site web. Dans ce cas, il y a de fortes chances que la photographie soit protégée par le droit d'auteur puisqu'il suffit qu'elle soit originale, ce qui est généralement reconnu par le juge. Or, il est unanimement admis que le fait de scanner (ou numériser d'une autre manière) une œuvre constitue un acte de reproduction, soumis au droit exclusif de l'auteur. Il en résulte que vous ne pourrez généralement ni scanner cette photo ni l'introduire sur votre site sans l'accord du photographe (ou d'une autre personne à qui il aurait cédé ses droits). En plus de cette

autorisation du photographe, vous devrez éventuellement obtenir l'autorisation de l'auteur de l'objet photographié ou de la personne photographiée.

Attention ! Ce n'est pas parce que vous avez acheté une photo ou les négatifs que vous êtes titulaire des droits d'auteur. Vous devez donc continuer à respecter ceux-ci.

51. Puis-je scanner une image (dessin) afin de l'inclure sur ma page web ?

De la même manière que pour les photos, vous serez peut-être tenté d'ajouter quelques images (telles que des images humoristiques ou de bandes dessinées) sur votre site en vue de le rendre plus attractif. Comme évoqué pour les photos, vous ne pourrez scanner une image et l'introduire sur votre site sans devoir demander l'autorisation de quiconque que si vous êtes le dessinateur de cette image, et pour autant qu'elle ne soit pas le portrait reconnaissable d'une personne.

Dans les autres cas, l'image sera protégée par le droit d'auteur si elle est originale, ce qui sera souvent le cas, et par conséquent vous devrez préalablement obtenir l'autorisation de l'auteur. Vous devrez également obtenir l'autorisation de la personne dessinée en vertu du droit à l'image. Indépendamment du droit d'auteur, il se peut aussi que l'image soit protégée par le droit des marques.

Une nouvelle fois, on voit que les hypothèses dans lesquelles vous pouvez exploiter – sans autorisation – une image sur votre site web sont rares, sauf à faire preuve de votre pouvoir créatif.

52. Puis-je scanner un texte afin de l'inclure sur ma page web ?

En plus des photos et des images, vous comptez mettre du texte sur votre site web. Ce texte, vous pouvez par exemple le rédiger vous-même ou vous allez peut-être scanner un texte existant et l'afficher sous forme d'image ou sous forme de texte, après avoir utilisé un logiciel de reconnaissance de caractères. Pouvez-vous introduire tout type de texte sur votre site ? Une nouvelle fois, la réponse est non.

En vertu des principes exposés ci-dessus, vous savez qu'un texte peut être protégé par le droit d'auteur s'il est original. Peu importe donc la longueur du texte (un slogan, quelques lignes ou plusieurs pages) ou le support sur lequel il est fixé au départ (papier, disquettes, CD-ROM, site en ligne, etc.).

Cela ne pose pas de problèmes si vous êtes l'auteur du texte, ce qui suppose que vous ayez inventé le contenu même du texte. Le fait de recopier un texte existant n'implique évidemment pas que vous deveniez l'auteur du texte.

Par contre, si le texte est protégé par le droit d'auteur, il ne pourra pas être reproduit sur le site sans le consentement de l'auteur (sauf à se prévaloir de l'exception de citation, *supra*, n° 47). En application de ce principe, la jurisprudence française a considéré comme une contrefaçon le fait d'avoir numérisé, sans l'autorisation des titulaires des droits, l'œuvre de Jacques Brel et de Michel Sardou. En Belgique, la jurisprudence a considéré que la reproduction d'articles de presse sur une base de données sur Internet constitue un acte nécessitant l'accord des auteurs.

53. Puis-je copier ou télécharger une œuvre (image, logo, icône, photo, texte, séquence vidéo, fichiers musicaux) d'un autre site afin de la placer sur mon site ?

L'hypothèse ici ne consiste plus à numériser une œuvre à partir d'un support analogique (un document papier) mais vise le cas où un site contient une œuvre (une image), et cette image est téléchargée par un internaute, qui la place sur son propre site et donc la (re)diffuse sur Internet.

La célèbre fonction *Copier/Coller* (*Copy/Paste*) offerte par la grande majorité des logiciels permet d'aller grappiller en quelques minutes une quantité impressionnante de données (sous forme de texte, d'image, de photo, etc.) qui se trouvent sur d'autres sites web. Encore une fois, cette fonction technique qui permet une reproduction aisée doit être utilisée avec modération et, en tout cas, dans le respect des droits d'auteur.

En effet, le fait de copier ou de télécharger une œuvre constitue un acte de reproduction et le fait de (re)diffuser cette œuvre sur Internet constitue une communication au public. Or ces actes sont couverts par le droit d'auteur. Il en résulte que si l'œuvre est protégée par le droit d'auteur, ce qui sera généralement le cas, vous devez en principe obtenir l'autorisation de l'auteur.

54. Puis-je scanner une image ou une photo sur support analogique ou copier une image ou une photo sur support numérique afin de l'installer sur mon site, même si je la modifie préalablement ?

Il existe sur le marché des logiciels de traitement d'images ou de dessin qui permettent de modifier une photo ou une image (changer la taille, les couleurs, les formes, le contraste, l'orientation, recadrer, etc.) d'une manière telle que l'image transformée peut ne plus avoir aucune ressemblance avec celle d'origine. Dans ce cas, êtes-vous dispensé de demander l'autorisation de l'auteur de l'œuvre d'origine (pour autant qu'elle soit protégée par le droit d'auteur, donc qu'elle soit originale) ?

NON, ce n'est pas parce que cette nouvelle image ne ressemble plus à l'image d'origine que vous pouvez faire n'importe quoi. En effet, pour pouvoir transformer cette image avec le logiciel *ad hoc*, vous avez préalablement accompli un acte de reproduction (soit par le fait de scanner l'œuvre soit par le fait de faire un *copier/coller*) qui nécessite une autorisation de l'auteur. De plus, le fait de retravailler l'image avec le logiciel de dessin relève non seulement du "droit d'adaptation", mais également du "droit à l'intégrité de l'œuvre", qui sont des droits exclusifs de l'auteur. Par conséquent, ces modifications nécessitent également l'autorisation de l'auteur.

Si l'image transformée ne ressemble plus du tout à l'image d'origine, comment l'auteur pourrait-il déceler l'infraction à ses droits et se prévaloir ainsi de ceux-ci ? Il est vrai qu'il sera souvent difficile pour un auteur de rechercher les atteintes à ses droits. Néanmoins, il faut savoir qu'il existe actuellement des systèmes de protection technique ("tatouage" ou "marquage" par exemple) qui permettent d'identifier une œuvre numérique, même si elle a été profondément modifiée et de la retrouver facilement sur Internet.

55. Puis-je mettre des fichiers musicaux (MP3 par exemple) à disposition des internautes sur mon site ?

Afin de traiter d'une question d'actualité et de simplifier le problème, nous nous limiterons aux fichiers musicaux au format MP3.

Qu'est-ce que le format MP3 ?

La norme MP3 est un standard de compression de données audio. Le format MP3 permet ainsi de compresser de 10 à 13 fois les fichiers sonores habituels, avec une perte de qualité qui est très minime. Il est donc possible de stocker le contenu de 10 à 13 CD "traditionnels" sur un seul CD au format MP3. On voit donc d'emblée les utilisations possibles sur Internet : alors qu'il fallait hier des heures pour télécharger une chanson de quelques minutes d'un chanteur quelconque, il ne faut plus aujourd'hui que quelques minutes si le fichier est au format MP3. Internet regorge de fichiers sonores (qui sont pirates dans la plupart des cas) au format MP3, soit parce qu'ils circulent d'un internaute à l'autre, soit parce que certains internautes enregistrent le contenu de leurs CD "traditionnels" sur leur ordinateur et compriment les fichiers à l'aide d'un logiciel *ad hoc* pour ensuite les diffuser sur le réseau.

Ce type d'acte est-il permis ?

Généralement, non ! Une composition musicale, comme toute autre création artistique ou littéraire, est protégée par le droit d'auteur si elle est originale, ce qui est souvent le cas. Ce n'est pas parce qu'on est sur Internet que ces principes ne sont plus d'application, même si l'ampleur de la fraude sur ce réseau semble donner l'illusion que le droit d'auteur ne s'applique pas.

Dès lors, si l'œuvre est protégée par le droit d'auteur, il est notamment interdit de numériser le contenu d'un vinyle ou d'un CD audio et de le copier sur son disque dur ou tout autre support (sauf si vous vous limitez à l'écouter dans le cercle familial). *A fortiori*, il est également interdit de le comprimer à l'aide d'un logiciel de compression MP3 et de rendre ces fichiers disponibles aux internautes par le biais de son site web sans l'autorisation du titulaire des droits sur les œuvres ainsi compressées. En effet, ces actes constituent des reproductions et une communication au public, qui relèvent des droits exclusifs de l'auteur. En application de ces principes, des tribunaux belges ou étrangers ont déjà condamné des personnes à plusieurs mois de prison. Ces dernières ont été reconnues coupables de contrefaçon, pour avoir construit un site permettant aux visiteurs de télécharger gratuitement des œuvres musicales pirates (au format MP3). De nombreuses sociétés (*telles que Napster et autres*) ont également eu des problèmes avec la justice pour avoir mis en place un logiciel et une plate-forme permettant aux internautes de s'échanger librement des fichiers MP3… généralement piratés.

Ne puis-je donc jamais introduire des fichiers MP3 sur mon site ?

Bien sûr que si. L'utilisation de la norme MP3 n'est comme telle pas interdite. Ce sont les conséquences de son utilisation sur le droit d'auteur qui posent problème. Il existe donc des cas dans lesquels le fait d'introduire un fichier MP3 sur son site web n'est pas répréhensible :

- soit parce que l'œuvre n'est pas originale et n'est donc par conséquent pas protégée par le droit d'auteur, mais autant dire que l'hypothèse est rare ;
- soit parce qu'on a soit même composé, interprété et enregistré l'œuvre. Dans ce cas, vous êtes en principe l'auteur et donc libre de la diffuser et de la reproduire comme bon vous semble ;
- soit parce que l'œuvre n'est plus protégée par le droit d'auteur car son auteur est décédé depuis plus de 70 ans. Mais attention, s'il ne faut pas demander d'autorisation au compositeur du morceau de musique ou de la chanson, des

autorisations peuvent être nécessaires de la part des musiciens (artistes interprètes) et des producteurs de phonogrammes ("Les maisons de disques"). De plus, il faut être prudent car il existe de nombreuses œuvres qui ne sont plus protégées par le droit d'auteur, mais dont l'arrangement l'est encore ;

- soit parce que les fichiers MP3 respectent les droits d'auteur.

56. Puis-je mettre des hyperliens renvoyant vers des sites qui contiennent des fichiers MP3 ?

La réponse est incertaine. Il n'existe pas de règle susceptible d'apporter une solution claire à cette question. Certaines juridictions ont décidé qu'il n'y avait rien d'illégal à établir un lien vers un matériel illicite (les fichiers MP3 pirates) tant qu'il ne se trouve pas sur son propre site. A l'inverse, d'autres ont adopté une solution moins souple. Vu l'incertitude, il est conseillé d'adopter une attitude prudente et de ne pas introduire sur son propre site des hyperliens vers des sites qui contiennent des fichiers MP3 (probablement pirates).

57. Si une œuvre n'est pas accompagnée de la mention "Copyright", puis-je la copier librement ?

Non, pas nécessairement. Le fait qu'une œuvre soit accompagnée ou non de la mention "*Copyright*" n'implique pas l'existence ou l'absence de la protection par le droit d'auteur. En effet, on a vu que la protection par le droit d'auteur existe par le seul fait de la création de l'œuvre et qu'il faut, et il suffit, que l'œuvre soit originale et mise en forme. Dès lors, ce n'est pas parce que l'œuvre n'est pas accompagnée de la mention "Copyright" que vous pouvez vous permettre de la copier librement. Vous devrez obtenir l'autorisation de l'auteur si l'œuvre est protégée.

Néanmoins, il est conseillé pour des questions de preuve d'indiquer la mention "*Copyright Dupont* – 2000" si vous intégrez sur votre site une de vos œuvres (texte, photo, etc.) qui bénéficie probablement de la protection par le droit d'auteur. En effet, selon l'article 6 de la loi sur le droit d'auteur, la personne qui apparaît comme telle sur l'œuvre du fait de la mention de son nom ou d'un signe quelconque est présumée titulaire des droits d'auteur.

58. Qu'en est-il des œuvres accompagnées de la mention "sans droit d'auteur" (Copyright free) ou prétendues "freewares" ou "sharewares" ?

On trouve fréquemment sur Internet des banques de données qui proposent des œuvres (photos, images ou logiciels) dont il est dit qu'elles sont "sans droit d'auteur" et qu'elles peuvent être reproduites librement. Pour les logiciels, on parlera aussi de "*freewares*" (ce sont des logiciels entièrement gratuits) ou "*sharewares*" (ce sont des logiciels distribués librement aux fins d'évaluation par l'utilisateur. Après une période d'essai, ce dernier doit contracter une licence ou arrêter d'utiliser le logiciel). La problématique est la même pour les logiciels dits "libres".

Ces mentions impliquent-elles nécessairement que ces photos, images ou logiciels ne sont pas protégés par le droit d'auteur ? La réponse est en principe négative. En effet, si l'œuvre est originale et que la durée des droits n'est pas expirée, elle est protégée par le droit d'auteur, et la déclaration des titulaires des droits selon laquelle elle est "libre de droit" (*Copyright free*) ne change rien à cette situation. Toutefois, on pourra considérer que ces titulaires donnent une licence gratuite d'utilisation.

Dans cette hypothèse, il faut être attentif à deux choses :

- D'une part, la licence d'utilisation ne signifie pas qu'on puisse faire n'importe quoi : les banques de données définissent généralement les types d'utilisations effectivement autorisées (on exclut par exemple les utilisations à des fins commerciales).

- D'autre part, le prétendu titulaire des droits peut ne pas être titulaire de ces droits. Dans ce cas, l'auteur en cause pourra se faire connaître et s'opposer à l'utilisation de son œuvre. La bonne foi de l'utilisateur ne pourra pas être opposée au titulaire des droits d'auteur (la bonne foi n'exclut pas la contrefaçon !).

59. Lorsque je renvoie, par hyperlien, vers un autre site web, dois-je obtenir l'autorisation du titulaire de ce site ?

Lorsque vous créez votre site web, vous allez probablement établir un ou plusieurs liens vers d'autres sites (ou vers une page particulière d'autres sites) (*supra*, n° 20). Dans ce cas, devez-vous demander l'autorisation du titulaire du site vers lequel vous établissez un lien hypertexte ?

Il semble que non. En général, ce type d'acte ne pose pas de problèmes au regard du droit d'auteur. Même si la question fait encore l'objet de discussions entre juristes, la tendance est de dire que tout responsable de site web est réputé avoir autorisé tacitement les autres opérateurs du réseau à établir un lien hypertexte pour autant qu'il soit simple et qu'il renvoie vers sa page d'accueil (et non une sous page du site web). Veillez néanmoins à vous abstenir d'introduire des hyperliens qui renvoient vers des sites ayant un contenu illicite ou préjudiciable (sites révisionnistes ou pornographiques par exemple).

Par contre, si vous utilisez d'autres techniques d'hyperliens qui ne sont pas considérées comme "simples", vous devez veiller aux implications juridiques éventuelles qui peuvent en résulter. A titre d'exemple, on cite l'hyperlien reprenant les titres (protégés par le droit d'auteur !) d'articles de presse et renvoyant systématiquement vers le site publiant ces articles. Cette pratique peut être jugée comme constituant de la concurrence déloyale (*parasitisme*) et/ou une violation du droit d'auteur. L'utilisation de "lien profond" peut aussi poser problème. Ce type d'hyperlien consiste à renvoyer vers une sous-page du site et donc à "court-circuiter" la page d'accueil. Certains responsables de site ont invoqué qu'il s'agissait d'une pratique préjudiciable notamment lorsque la page d'accueil est la seule à contenir des bannières publicitaires qui, par l'effet du lien profond, ne pouvaient pas être vues par de nombreux internautes. L'utilisation de la technique du *framing* (utilisation de cadres, de fenêtres) combinée aux hyperliens doit également faire l'objet d'une certaine vigilance. Vous devez éviter de la sorte d'induire le public en erreur sur le titulaire réel du site. En effet, on peut imaginer que vous introduisiez un hyperlien dans une fenêtre (*frame)* qui renvoie vers un splendide poème sur un autre site. Lorsque l'on clique sur ce lien, il peut arriver que la page contenant ce poème apparaisse de manière telle que l' internaute ne se rende pas compte qu'il est sur un autre site et croie à tort que le poème est de vous. Abstenez-vous de ce genre de pratique ou veillez à obtenir l'autorisation du responsable du site référencé.

60. Puis-je m'opposer à ce que l'on établisse un lien hypertexte vers mon site ?

Comme expliqué dans la réponse à la question précédente, on considère généralement que le responsable d'un site web est réputé avoir autorisé tacitement les autres opérateurs du réseau à établir un lien hypertexte vers son site.

Toutefois, un sérieux bémol doit être apporté à ce principe. Vous pourrez toujours vous opposer à un hyperlien qui renvoie vers votre site si celui-ci est fait dans un contexte qui

vous est préjudiciable. Il en serait par exemple ainsi pour un hyperlien renvoyant à votre site qui se trouverait pour une raison ou une autre sur un site web à caractère pornographique ou révisionniste, ou qui serait intégré dans une phrase ayant un contenu dénigrant ou insultant. L'hyperlien pourrait aussi, suivant le contexte, être jugé comme de la publicité trompeuse (qui est interdite) ou comparative (mais qui ne respecterait pas l'ensemble des conditions de la loi). Serait également jugé préjudiciable un hyperlien qui profiterait par trop de votre travail (vous avez créé un site publiant vos photos inédites dans le domaine de l'alpinisme, et un autre utilisateur créerait un site, vide de contenu, mais renvoyant systématiquement par hyperlien vers les photos localisées sur votre site, le tout dans une certaine confusion).

Vu les conséquences préjudiciables qui peuvent résulter de l'utilisation d'hyperliens, certains sites indiquent dans leurs conditions générales la clause suivante, afin de prévenir le problème : "Tout utilisateur s'engage à demander l'autorisation du responsable de ce site web avant d'établir un hyperlien, de quelque nature qu'il soit, vers celui-ci" ou encore "L'insertion sans autorisation de liens directs sur cette page, sur des fichiers ou des applications de ce site est interdite".

61. Quelles sont les sanctions en cas de non respect du droit d'auteur ?

Le non respect des principes évoqués ci-dessus peut être passible de sanctions pénales (peines de prison ou d'amende) et/ou de sanctions civiles (paiement de dommages et intérêts par exemple).

Il faut souligner que la contrefaçon n'implique pas de volonté de nuire, ni même la connaissance du droit d'autrui sur l'œuvre. Il n'est donc pas possible de se retrancher derrière son ignorance de bonne foi pour éviter une condamnation.

En outre, le juge peut ordonner qu'une publication du jugement soit faite à charge du contrevenant, dans la presse ou un autre média (par exemple sur la *homepage* d'un site web). Les objets qui ont été contrefaits peuvent être confisqués.

Ces sanctions peuvent apparaître théoriques étant donné que la fraude sur Internet a pris une ampleur colossale et que le risque de se faire prendre est minime. Détrompez-vous ! Des mécanismes techniques sont de plus en plus utilisés en vue d'identifier les œuvres protégées et de traquer, à l'aide de moteurs de recherche automatisés, les fraudes sur Internet. De plus, des organisations professionnelles ou des sociétés de gestion collective de droits d'auteur n'hésitent plus à mettre tout en œuvre en vue de faire respecter les droits de leurs membres. Enfin, de nombreuses juridictions, notamment belges et françaises, ont déjà condamné pour contrefaçon des personnes ayant affiché sur leur site des œuvres protégées par le droit d'auteur. A bon entendeur…

62. Mon site est-il protégé par le droit d'auteur ou un autre droit ?

On a vu précédemment que lorsque vous créez un site web, vous devez le faire dans le respect du droit des tiers et notamment des droits d'auteur. A l'inverse, vous pouvez être intéressé à ce que votre propre site web ainsi que son contenu soient protégés. En effet, si vous êtes photographe amateur et que vous désirez permettre aux internautes de consulter vos clichés, vous n'avez pas nécessairement envie qu'un tiers vienne copier l'ensemble de vos photos en vue de créer un site analogue. Ce qui est vrai pour des photos est également vrai pour des poèmes, des compositions musicales et des publications scientifiques ou autres. D'autre part, la structure de votre site peut être en elle même originale et vous aimeriez en garder la paternité.

Vu la complexité de la matière, nous ne rentrerons pas dans les détails. Vous devez néanmoins savoir que le contenu de votre site (textes, images, photos, etc.) peut être protégé par le droit d'auteur pour autant que vous soyez l'auteur de ce contenu. De plus, le site lui même (c'est-à-dire sa présentation, mise en page, typographie, dessins, structure des éléments) peut également être protégé par le droit d'auteur, comme ce sera expliqué ci-après. La seule condition est que le site et son contenu soient originaux (*supra*, n° 42), ce qui sera généralement le cas. A ce titre, vous pourrez donc vous opposer à toute reproduction par un tiers de ces éléments.

De plus, une directive européenne du 11 mars 1996, transposée par la loi belge du 31 août 1998 (*M.B.*, 14 novembre 1998, p. 36914), institue une double protection pour les bases de données d'une part, par le droit d'auteur, d'autre part, par un droit spécifique nommé droit "*sui generis*".

Le droit d'auteur protège la base de données (un site web peut être considéré comme une base de données ou à tout le moins contenir une base de données) originale, c'est-à-dire celle qui, par le choix ou la disposition des matières, constitue une création intellectuelle propre à son auteur. La protection s'applique non au contenu de la base de données (qui reste protégé le cas échéant par un droit d'auteur spécifique ou un autre droit tel par exemple le droit des marques), mais bien à la structure de celle-ci. Le titulaire du droit est le créateur de la base de données (qui peut être une personne physique ou morale). La durée du droit est identique à la durée du droit d'auteur traditionnel, soit 70 ans après la mort de l'auteur.

Les bases de données (surtout si elles sont non originales) peuvent également jouir d'une protection instituée par le droit *sui generis* qui s'applique aux bases de données dont l'obtention, la vérification ou la présentation du contenu atteste un investissement substantiel du point de vue quantitatif ou qualitatif. Le titulaire du droit est le producteur de la base de données qui est défini comme la personne physique ou morale qui a pris l'initiative et le risque de l'investissement. Le droit qui lui est reconnu est celui d'empêcher l'extraction et/ou la réutilisation de la totalité ou d'une partie substantielle de la base de données (ou de l'autoriser moyennant rémunération). La durée du droit est de 15 ans à compter de la fabrication de la base de données. Chaque modification substantielle de celle-ci permet en outre de bénéficier d'une nouvelle période de protection de 15 ans.

Partie 4.
Se protéger des “agressions” sur Internet

CHAPITRE I. LES ATTEINTES A LA VIE PRIVEE

Section 1. Les techniques d'intrusion

63. En quoi ma vie privée est-elle menacée lorsque je "surfe" sur Internet ?

Se connecter à Internet est devenu pour beaucoup d'entre nous un geste quotidien, plutôt banal : envoi d'e-mails, visite de sites web, discussion en temps réel dans des *chatrooms*, etc.

A chaque connexion, Internet nous donne une impression de liberté et d'anonymat, mais en réalité, il en va tout autrement. En effet, lorsque vous "surfez" sur Internet, vous dévoilez des informations vous concernant en laissant un certain nombre de traces. En général et par défaut, toute une série d'éléments sont automatiquement transmis au site que vous visitez par le logiciel de navigation que vous utilisez :

- l'adresse TCP/IP, c'est-à-dire un numéro unique au monde attribué à votre micro-ordinateur sur le réseau ;
- la marque et la version de votre navigateur ainsi que celles de votre système d'exploitation ;
- la langue utilisée ;
- la dernière page web consultée (s'il y avait un lien que vous avez suivi vers la page actuelle) ;
- les *cookies* rémanents (*infra*, n° 64) déjà envoyés par le site visité.

Ces différentes informations sont rendues automatiquement accessibles au serveur web et lui permettent de prendre en compte des éléments propres à la configuration utilisée par l'internaute. Connaître, par exemple, le type de navigateur et sa version peut permettre au serveur de ne pas lancer certaines applications qui seraient incompatibles avec lui.

En termes de protection de la vie privée, le problème naît de l'association de ces variables avec les autres informations vous concernant que le serveur a pu glaner ailleurs (par exemple via son fournisseur d'accès), et ce, sans que vous en ayez été informé et mis en mesure de vous y opposer. Ainsi, si vous remplissez un formulaire en ligne comportant des informations personnelles, le lien entre l'adresse TCP/IP de votre ordinateur et ces informations peut être fait sans difficulté de sorte que votre parcours sur le site peut être suivi, dans le but de conduire à la constitution d'un profil précis.

Diverses techniques permettent ainsi de recueillir, de manière invisible, vos informations personnelles afin d'observer vos habitudes sur Internet. Prises individuellement, chacune de ces techniques ne permet de collecter qu'une quantité limitée d'informations. Elles sont donc relativement peu "privacides", mais elles peuvent l'être davantage lorsqu'elles sont utilisées en combinaison avec d'autres méthodes. Elles deviennent alors de puissants outils d'observation qui servent actuellement à des fins de marketing mais pourraient être utilisées à des fins de discrimination ou de modification de l'information transmise.

Parmi ces techniques, la plus répandue est l'usage de *cookies* enregistrant votre parcours sur Internet (*infra*, n^{os} 64 et s.). Certaines techniques sont plus vicieuses et peuvent même porter atteinte à la sécurité des données personnelles situées sur votre disque dur comme les espiogiciels (*infra*, n^{os} 69 et s.).

Pour découvrir comment vous êtes “pisté” sur Internet, visitez le site de la Commission Nationale Informatique et des Libertés : http://www.cnil.fr (équivalent français de notre Commission pour la protection de la vie privée).

64. Qu’est-ce qu’un “cookie” ?

Un *cookie* est un fichier informatique au format texte envoyé et enregistré sur votre ordinateur par un serveur web lors de la consultation d’un site Internet. Le *cookie* permet au serveur web de conserver sur votre ordinateur des données auxquelles il pourra accéder lorsque des visites de ce site Internet seront effectuées à partir de la machine sur laquelle ce *cookie* a été enregistré.

Pratiquement, le serveur envoie un ou plusieurs *cookies* à votre programme de navigation. Votre navigateur recevant un *cookie* le stocke dans un fichier particulier situé sur votre ordinateur. Par la suite, votre navigateur le communiquera systématiquement lorsque vous ferez une requête au même serveur que celui ayant transmis le *cookie* initial. Mais il est possible qu’un *cookie* soit partagé entre plusieurs serveurs d’un même domaine.

On distingue les *cookies* de session et les *cookies* rémanents.

Les *cookies* de session ne contiennent pas de date d’expiration, ne sont pas écrits sur votre disque dur et sont automatiquement détruits lorsque vous fermez la session ouverte sur le site web. Ils sont généralement créés pour des raisons techniques (sans les *cookies* de session, lorsque vous êtes sur un site et passez d’une page à l’autre en cliquant sur des liens hypertextes, chaque requête serait traitée de manière complètement indépendante comme s’il s’agissait d’utilisateurs différents accédant à une seule page du site). Ils n’ont pas pour objectif d’instaurer un lien permanent entre votre machine et le site consulté.

Par contre, les *cookies* rémanents contiennent une date d’expiration fixée par le serveur et sont destinés à permettre à celui-ci d’accéder aux informations qu’ils contiennent jusqu’à l’échéance de ce terme.

La durée de vie d’un *cookie* est variable selon la volonté du serveur source ; quelques minutes, le temps d’une connexion, ou plusieurs années (35 ans maximum).

65. A quoi sert un “cookie” ?

Les *cookies* peuvent constituer des instruments précieux pour améliorer le confort de la consultation, notamment en permettant de gagner en rapidité.

Les *cookies* peuvent êtres utilisés à des fins très diverses.

Dans un certain nombre de cas, le serveur a besoin d’identifier qui est le visiteur. Par exemple, la plupart des sites de commerce en ligne permettent de constituer une sorte de panier d’achats virtuels avant passation de la commande. L’internaute surfe sur le site et choisit progressivement les articles qu’il veut commander. Ceux-ci sont emmagasinés dans le panier ; l’état de celui-ci est entretenu par des mécanismes à base de *cookies*. Dans le cas d’un site multilingue, il peut être intéressant de retenir qu’une personne est francophone pour afficher directement les pages en français lorsqu’elle visite le site. A cette fin, le serveur va déposer sur le disque dur de la personne concernée un *cookie* qui indiquera cette particularité ; lors des consultations ultérieures, le serveur ira d’abord lire le *cookie* et déduira la langue d’affichage. En cas de rupture de connexion pendant la transaction, le *cookie* permettra au vendeur de retrouver votre trace grâce au *cookie* précédemment installé sur votre ordinateur.

Le *cookie* permet également de prendre en compte vos habitudes et de vous envoyer des informations sur mesure. En effet, les *cookies* permettent à un serveur de déterminer votre parcours durant une session et de vous "profiler" en conséquence. Il suffit pour cela au serveur de positionner un *cookie* à chaque page ou lors de chaque action que vous faites puis de les récupérer globalement afin d'analyser votre parcours. Rien n'empêche alors de vous proposer des pages créées dynamiquement en fonction de votre profil.

L'effet pervers de cette technique est qu'elle peut se révéler très indiscrète. Il ne faut pas perdre de vue que des informations peuvent ainsi être collectées à votre insu par certains gestionnaires de sites ou des entreprises publicitaires. En effet, lors de la visite d'un site web, des informations relatives par exemple aux pages visitées, aux préférences en matière de langue, à la nature des recherches effectuées sur un moteur de recherche, vont être stockées sur le *cookie* et renvoyées au gestionnaire du site lors de chaque nouvelle visite.

Les informations contenues dans le *cookie* peuvent ainsi servir à constituer un profil de plus en plus précis de vos habitudes et de vos préférences, ce qui permettra au gestionnaire du site de vous proposer des produits censés correspondre à vos goûts. Le *cookie* peut donc se révéler un outil intéressant pour les sociétés de marketing direct afin de cibler vos centres d'intérêts et d'enregistrer dans des bases de données vos habitudes de consommation.

66. Dois-je me méfier des cookies ?

En principe, on ne peut disposer par le biais des *cookies* d'informations que vous n'auriez pas transmises précédemment d'une manière ou d'une autre. Par conséquent les *cookies* ne permettent pas en tant que tels de connaître votre nom ou votre adresse e-mail.

Cependant, si vous n'êtes pas toujours clairement identifié, vous êtes à tout le moins identifiable. En effet, vous ne devez pas perdre de vue que tous les *cookies* positionnés dans votre ordinateur et auxquels vous ne prêtez pas attention peuvent être mis en relation avec des informations plus précises (données nominatives) que vous aurez transmises un jour ou l'autre, par exemple en remplissant un formulaire. Il en est de même de toutes les informations sur les logiciels que vous utilisez, les informations bancaires ou les autres informations qui auront été spontanément données par vous-même. Un tel recoupement d'informations permet de constituer de véritables bases de données comportementales, et cela, totalement à votre insu !

Sachez enfin que chaque *cookie* est une trace qui reste sur le disque dur et qui indique votre cheminement sur Internet. Dès lors, lorsque vous effectuez votre session à partir d'un ordinateur qui n'est pas le vôtre, prenez vos précautions si vous n'avez pas envie que cette visite soit connue de l'utilisateur suivant.

67. Comment se protéger des cookies ?

Selon votre degré d'agacement face à cette intrusion dans votre vie privée, vous disposez de différentes options pour freiner, voire stopper l'invasion. Cependant, aucune solution n'est tout à fait idéale.

Vous pouvez d'abord activer la fonction d'alerte de votre navigateur. Les principaux programmes de navigation (Netscape Navigator et Microsoft Explorer) permettent de signaler "en temps réel" l'arrivée de *cookies*. A ce moment, vous pouvez accepter ou refuser l'enregistrement du *cookie*. Bonne idée certes, car vous pourrez ainsi accepter les *cookies* qui vous seront utiles et voir quels sites cherchent à vous épier. Hélas, dans la

pratique, cette solution devient vite pénible. Vous découvrirez que le nombre de sites envoyant des *cookies* est faramineux. Par conséquent, votre surf sera constamment pollué par les alertes au *cookie* de votre navigateur. Mais c'est la rançon d'un contrôle efficace…

En outre, sachez que, par défaut, la protection n'est pas activée et les connaissances techniques nécessaires pour l'activation ne sont pas évidentes. Pour être averti de l'envoi d'un *cookie*, vous devez paramétrer votre navigateur.

Certaines versions de navigateurs vous offrent la possibilité de refuser d'office les *cookies*. Vous pouvez configurer votre navigateur pour qu'il refuse automatiquement l'intrusion de *cookie*. Hélas, cette solution radicale n'a pas que des conséquences heureuses. Les sites web où vous avez vos habitudes ne vous reconnaîtrons plus. Il vous faudra alors saisir vos données d'utilisateur à chaque fois. Autre détail important : vous ne pourrez pas, dans certains cas, effectuer des achats en ligne. En outre, certains sites vous bloqueront l'accès si vous n'acceptez pas leurs *cookies*. Cette solution est la plus efficace du point de vue de la protection de votre intimité, mais elle perturbera quelque peu votre surf et limitera votre champ d'action.

Vous pouvez également détruire les *cookies*. Il est possible de localiser l'endroit où sont stockés les *cookies* sur votre disque dur. Une fois localisés, il vous suffit de supprimer les *cookies* non désirés. Nous vous déconseillons de mener une telle opération régulièrement, car si vous revenez sur les sites qui vous ont "collé" des *cookies* la semaine précédente, de nouveaux fichiers vous seront envoyés. Un cercle vicieux… Par ailleurs, vous risquez d'éliminer aussi les *cookies* utiles : ceux qui contiennent des informations de personnalisation pour les accès à des sites que vous fréquentez régulièrement. Lorsque vous accéderez à ces sites, le navigateur vous demandera de saisir à nouveau certaines informations : nom d'utilisateur, mot de passe... La solution manuelle a donc du bon, mais uniquement pour ceux qui n'utilisent pas de services sur le *net* (mail, shopping, enchères, etc.).

D'autres parades existent. Vous pouvez avoir recours à des programmes "tueurs de *cookies*", téléchargeables gratuitement sur Internet. Une autre solution réside dans l'utilisation d'un proxy serveur (http://www.inetprivacy.com) : il s'agit d'un serveur HTTP qui sert d'intermédiaire entre l'internaute et le réseau, effectue les requêtes HTTP en son nom et lui communique les résultats. Vous n'êtes donc pas, dans ce cas-là, identifié par votre correspondant. La solution du proxy serveur demande un minimum de connaissance technique pour son installation et n'est gratuite que dans sa version de démonstration.

68. Comment me protéger juridiquement ?

La loi belge réglemente l'usage de vos données à caractère personnel (*infra*, n^{os} 72 et s.). Une donnée à caractère personnel est une information concernant une personne physique identifiée ou identifiable. Le *cookie*, lorsqu'il permet de vous identifier (également par recoupement avec d'autres fichiers, etc.), peut être considéré comme une donnée à caractère personnel.

Dans ce cas là, certaines règles doivent être respectées :

- l'auteur du site doit vous informer avant de stocker un *cookie* sur votre disque dur ;
- l'auteur du site doit dévoiler son identité (pas seulement son URL ou son adresse *e-mail*, mais aussi ses coordonnées) ;
- l'auteur du site doit déterminer dans quel but le *cookie* sera utilisé ;
- l'auteur du site doit signaler l'existence d'un droit d'accès ;
- l'auteur du site doit permettre le droit d'accès ;
- l'auteur du site doit permettre un droit d'opposition.

69. Qu'est-ce qu'un espiogiciel ?

Aussi appelé *spyware* ou logiciel espion, l'espiogiciel est un petit programme informatique le plus souvent intégré ou livré en complément d'un logiciel principal. Les espiogiciels se trouvent généralement dans le code d'un programme que vous téléchargez innocemment sur Internet. Dans la plupart des cas, ces espiogiciels sont des "petits morceaux de codes parasites" (routines) intégrés dans le code principal du programme. Dans un même programme, il peut y avoir plusieurs routines parasites différentes, ayant chacune une fonction déterminée.

La détection de ces routines est très malaisée. Dans tous les cas, l'espiogiciel aura besoin d'une connexion Internet pour la transmission des données. C'est pourquoi, les espiogiciels sont fréquemment associés à des logiciels proposés en téléchargement sur Internet (logiciels de téléchargement de fichiers MP3, films, traducteurs, *browsers*, etc.). Généralement les logiciels libres (*freewares*) et logiciels d'évaluation (*sharewares*) sont les principaux vecteurs d'espiogiciels.

Les espiogiciels s'installent sur un ordinateur comme les autres programmes, généralement sans que vous en ayez connaissance ou soyez informé de leur finalité, et collectent des données sur votre comportement d'internaute et votre machine.

On peut également considérer comme mouchards *les web bugs* qui prennent la forme d'une image invisible et indétectable constituée d'un unique pixel inséré dans des pages ou courriers électroniques au format HTML. Ces derniers toutefois ne font pas l'objet d'une installation permanente sur les machines des utilisateurs concernés. Ils sont le plus souvent utilisés à des fins de mesure d'audience.

70. A quoi sert un espiogiciel ?

Véritables mouchards électroniques, au même titre que les *cookies* mais aux fonctionnalités beaucoup plus étendues, ils peuvent envoyer dès le démarrage de l'ordinateur vers les serveurs d'un organisme "maître" toutes les données qu'ils ont collectées, comme les habitudes de navigation et les adresses de tous les sites visités.

En outre, l'espiogiciel peut représenter une très grande menace pour la sécurité du système informatique infecté. Il peuvent servir à prendre connaissance de la configuration exacte de l'ordinateur et du contenu de son disque dur ; plusieurs routines successives peuvent permettre la détection de mots de passe encryptés et le crackage de ces informations.

La fonction essentielle d'un espiogiciel est, sous couvert ou non d'un autre service, de transmettre ces données à son créateur, la plupart du temps à des fins de ciblage publicitaire et commercial. Ces données constituent une ressource appréciable pour les entreprises, la valeur de leurs fichiers et de leurs bases de données étant déterminée par la qualification et le profilage le plus précis possible des internautes listés.

En marge des questions liées à la protection de la vie privée, il faut enfin remarquer que les espiogiciels mobilisent des ressources de l'ordinateur lorsqu'ils sont actifs en tâche de fond (mémoire disque, mémoire vive et bande passante pour les transmissions de données).

71. Comment se protéger des espiogiciels ?

Se protéger des *spywares* n'est pas chose facile. En pratique, plusieurs mesures peuvent être adoptées par l'internaute pour se prémunir contre les effets non désirés des espiogiciels.

Il convient tout d'abord de prendre garde à ce que vous installez sur votre ordinateur. La plus grande vigilance est notamment recommandée dans le cas de nombreux logiciels distribués gratuitement. Une des caractéristiques majeure des espiogiciels est qu'ils sont souvent installés à l'insu de l'utilisateur. Les boîtes de dialogue d'installation offrent rarement la possibilité de refuser ces fonctionnalités. Lorsqu'une installation personnalisée d'un logiciel est proposée, vous désactiverez les modules additionnels qui ne sont pas absolument nécessaires au fonctionnement du logiciel. Un certain discernement quant aux actions à effectuer, propre aux utilisateurs avertis, est cependant nécessaire.

Une seconde précaution élémentaire consiste à lire attentivement le contrat de licence d'utilisateur final qui contient généralement en toutes lettres la mention de l'intégration de fonctionnalités de *spyware* dans le logiciel que vous vous apprêtez à installer. Le choix d'un logiciel concurrent disposant de fonctionnalités équivalentes mais dépourvu d'espiogiciel pourra alors constituer une bonne alternative.

L'usage d'un logiciel antivirus et d'un pare-feu (*firewall*) peut s'avérer utile. Toutefois, leur efficacité est très relative. Le *firewall*, sauf exception, n'a pas pour but d'analyser ce qui sort du PC, mais à l'inverse ce qui y rentre. Certains pare-feux permettront par exemple à l'utilisateur d'être alerté des tentatives de connexion à des serveurs distants. L'antivirus, quant à lui, ne risque pas d'avoir beaucoup d'effet car les espiogiciels ne sont pas considérés ni répertoriés comme des virus et passent souvent au travers de ces filtres.

Le moyen le plus efficace de se prémunir contre les espiogiciels est d'avoir recours à des programmes permettant de les identifier et de les mettre hors d'usage ou de les détruire. Certains sites listent ainsi les espiogiciels connus et les programmes anti-*spyware*, disponibles gratuitement sur Internet, dont l'efficacité paraît satisfaisante (voir http://www.spychecker.com). Aucun site, cependant, ne peut prétendre avoir une liste exhaustive des espiogiciels existants. De même, certains outils permettent la détection de logiciels identifiés comme ayant des *spywares* mais les utiliser ne garantit pas une sécurisation à 100% de votre ordinateur. En outre, l'usage de ces techniques de protection est réservé à des utilisateurs confirmés, une mauvaise manipulation des logiciels ou des effacements malencontreux de fichiers pouvant être préjudiciables au bon fonctionnement de la machine. En cas de doute, n'hésitez pas à vous entourer des conseils de personnes qualifiées en informatique.

Section 2. La protection de la vie privée et le traitement des données à caractère personnel

72. Qu'est-ce qu'un traitement de données à caractère personnel ?

Si les nouvelles technologies de l'information et de la communication offrent de grandes possibilités et de nombreux avantages, elles présentent également de nouveaux dangers pour la vie privée et les libertés de chacun.

Dans un grand nombre de cas, l'information qui circule sur Internet se rapporte à des personnes. Des bases de données ou des fichiers reprenant vos informations personnelles sont constitués, utilisés, communiqués et vendus. Il est désormais difficile de savoir qui sait quoi sur vous et qui en fait quoi. L'individu a en quelque sorte perdu la maîtrise de l'information qui le concerne. Face à ce phénomène, la Belgique, comme les autres pays de l'Union européenne, dispose d'une législation sur la protection de la vie privée qui réglemente le traitement par autrui de vos données personnelles.

Une *donnée à caractère personnel* est une information qui vous identifie ou qui permet de vous identifier. Votre nom et votre adresse (même celle de votre lieu de travail) sont considérés comme des données à caractère personnel, tout comme votre adresse électronique.

Cette notion vise également toute une série d'informations qui permettent de vous identifier de manière indirecte (par recoupement), notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques propres à votre identité physique, psychique, économique, culturelle ou sociale. Il peut s'agir du numéro d'immatriculation de votre véhicule, de données contenues dans un répertoire d'adresses professionnel ou non, de photos, de données invisibles transmises lors de sessions Internet (adresses IP), de données bibliographiques, etc.

Pour que s'applique la législation de protection des données à caractère personnel, il faut être en présence d'un *traitement* de telles données. Cette notion vise toute opération ou ensemble d'opérations appliqués à des données personnelles. Les opérations dont il s'agit sont particulièrement variées et comprennent la collecte de données, leur conservation, leur utilisation, leur modification, leur transmission, etc. Par exemple, chaque fois que vous êtes invité à remplir un formulaire en ligne, cela correspond à un traitement de données pour celui qui va les recueillir. De même, l'hôtel qui offre la possibilité de faire une réservation via Internet réalise un traitement de données lorsqu'il enregistre votre nom, les dates de votre séjour et votre numéro de carte de crédit.

La loi s'applique dès que les opérations sont effectuées sur des données à caractère personnel en tout ou en partie à l'aide de procédés automatisés (cela englobe toutes les technologies de l'information : informatique, télématique, réseaux de communication). Cela concerne, par exemple, une base de données informatiques où sont enregistrés les clients d'une société, la liste électronique des opérations effectuées sur un compte en banque, le fichier informatisé du personnel d'une entreprise, etc.

La loi s'applique également si ces opérations se font sans le moindre recours à des procédés automatisés, dès lors que les données sur lesquelles portent la ou les opérations sont contenues ou appelées à figurer dans des *fichiers* (c'est-à-dire un ensemble structuré dans lequel les données sont accessibles selon des critères spécifiques, comme l'ordre alphabétique).

73. Comment savoir qui est le responsable du traitement de mes données ?

Il est très important que vous sachiez qui, aux yeux de la loi, est considéré comme le "responsable du traitement". C'est en effet sur cette personne que repose la charge de presque toutes les obligations imposées par la loi pour assurer la protection des données traitées. C'est donc lui qui sera tenu responsable si un problème survient ; il est votre interlocuteur principal.

La loi désigne comme responsable du traitement la personne qui, seule ou conjointement avec d'autres, détermine les finalités (par exemple, la collecte de données à des fins de constitution de profils marketing) et les moyens du traitement de données à caractère personnel (formulaires en ligne, *cookies*, etc.). Il s'agit donc de la personne investie du pouvoir de décision sur le traitement de données.

Lorsque quelqu'un récolte des données sur vous, il a l'obligation de vous communiquer le nom du responsable de traitement ainsi que le type de traitement qu'il opère. Le cas échéant, vous pouvez vous adresser à la *Commission de la protection de la vie privée*, qui a notamment pour mission de tenir à jour un registre public reprenant ces informations.

74. Quels sont les droits que je peux exercer pour protéger ma vie privée ?

Dès lors que vos données font l'objet d'un traitement, la loi sur la protection de la vie privée vous protège et vous reconnaît des droits :

1. Le droit à l'information

De manière générale, la loi vous confère "un droit de savoir", c'est-à-dire le droit d'être informé du sort réservé aux données vous concernant. Ainsi, des fichiers ne peuvent être constitués à votre insu.

Tout responsable de traitement est tenu de fournir certaines informations aux personnes concernées par les données. Il doit notamment vous communiquer ses nom et adresse, le but dans lequel il récolte vos données et les destinataires de ces données. Il doit également vous informer de vos droits (accès, rectification, opposition, etc.).

Ce devoir d'information incombant au responsable du traitement doit être accompli soit au moment de l'obtention des données, lorsqu'il les a obtenues de vous-même, soit au plus tard au moment de la première communication de ces données, lorsque celles-ci ont été obtenues de manière indirecte.

Notons en outre, que les données qu'on vous demande de livrer doivent être pertinentes au vu des finalités pour lesquelles elles sont récoltées. L'obtention de votre numéro de téléphone privé, par exemple, n'est bien souvent pas nécessaire pour atteindre les finalités annoncées.

2. Le droit à la curiosité

Vous avez le droit d'interroger tout responsable de traitement pour savoir s'il détient des données vous concernant. Le responsable interrogé doit confirmer ou non s'il détient de telles données et, dans l'affirmative, il doit préciser dans quel but il les détient, de quelles catégories de données il s'agit et quels en sont les destinataires.

3. Le droit d'accès

Vous avez le droit d'obtenir, sous forme intelligible, une copie des données faisant l'objet d'un traitement ainsi que toute information disponible sur l'origine des données.

Pour exercer votre droit d'accès, il vous faut adresser une demande au responsable du traitement en faisant la preuve de votre identité. Le responsable doit répondre, sous peine d'amende, au plus tard dans les 45 jours de la réception de la demande.

4. Le droit de rectification

Les données vous concernant qui sont collectées doivent être exactes. Le cas échéant, le responsable du traitement doit donc vous offrir des moyens raisonnables pour rectifier, effacer ou bloquer ces données.

5. Le droit d'opposition

Sauf lorsque le traitement est nécessaire à la conclusion ou à l'exécution d'un contrat ainsi qu'au respect d'une obligation légale, vous avez le droit de vous opposer au traitement de vos données, mais pour cela, vous devez invoquer des raisons sérieuses et légitimes tenant à votre situation particulière.

En outre, sachez que l'utilisation de données personnelles dans le cadre d'opérations de marketing direct est strictement réglementée. Dès lors, la loi vous offre toujours la possibilité de vous opposer, sans justification et gratuitement, au traitement projeté lorsque des données à caractère personnel sont collectées à des fins de marketing direct (*infra*, n^{os} 85 et s.).

6. Le droit à l'oubli

Les données permettant l'identification des personnes ne doivent pas être conservées au-delà du délai nécessaire à la réalisation de la finalité annoncée.

75. Quels sont les recours si mes droits ne sont pas respectés ?

Vous pouvez vous adresser sans frais à la *Commission de la protection de la vie privée*, qui procédera aux vérifications nécessaires. Vous trouverez les renseignements concernant cette institution à l'adresse suivante : http://www.privacy.be.

Vous pouvez en tout état de cause soumettre votre litige aux cours et tribunaux.

76. Mes données personnelles sont-elles protégées en dehors de l'Union européenne ?

Le caractère international du réseau a pour conséquence une circulation fréquente des données à caractère personnel des particuliers entre différents pays, parfois sans que la destination des données soit même identifiée par l'utilisateur.

En principe, on ne peut transférer vos données personnelles que vers des pays qui assurent une protection des données correspondante à celle assurée sur le territoire de l'Union européenne.

Tout responsable de traitement qui souhaite *exporter des données personnelles hors de l'Union européenne* doit dès lors se demander si le pays destinataire offre un niveau de protection adéquat. Il faut retrouver les mêmes garanties que celles établies sur le territoire européen. Dans le cas contraire, le transfert ne pourra être effectué que moyennant le strict respect de certaines conditions. Tel sera le cas si le responsable du traitement obtient votre consentement indubitable au transfert ou encore si des garanties sont offertes par l'adoption de clauses contractuelles appropriées entre l'exportateur et l'importateur de données.

Lorsque les *données sont collectées en Belgique à partir d'un pays tiers*, les dispositions de la loi belge trouvent à s'appliquer dans des circonstances précises. Ce sera le cas notamment lorsque le responsable du traitement fait traiter les données à caractère personnel, par des moyens automatisés ou non, situés sur le territoire belge. L'utilisateur résidant en Belgique peut dans une telle hypothèse bénéficier de la protection offerte par la loi belge vis-à-vis du responsable de traitement.

Section 3. La cybersurveillance sur le lieu de travail

L'informatique a envahi progressivement les entreprises, ce qui n'a pas manqué d'entraîner certaines conséquences au niveau de la relation existant entre le travailleur et l'employeur.

Pour l'entreprise, les nouvelles technologies posent de nouveaux problèmes en matière de sécurité puisque des informations sur toute la vie de l'entreprise sont plus facilement susceptibles de sortir du cadre de celle-ci. En outre, l'employeur doit pouvoir vérifier la bonne exécution du contrat de travail.

Pour les employés, la difficulté réside dans la capacité qu'a la société d'identifier et de conserver toutes les traces laissées par la personne connectée et, ainsi, de mettre en place une surveillance qui porte atteinte au respect de sa vie privée.

L'équilibre entre les exigences de rentabilité et de sécurité des entreprises, d'une part, et la préservation d'un espace d'épanouissement individuel sur le lieu de travail, d'autre part, est particulièrement délicat à trouver.

77. Quels sont les grands principes ?

Il est admis aujourd'hui que le travailleur bénéficie d'une sphère de vie privée sur son lieu de travail, et à ce titre, d'une certaine protection contre un contrôle intempestif de la part de l'employeur de l'usage qu'il fait des moyens de communications mis à sa disposition pour l'exécution de son contrat de travail.

Néanmoins, la réglementation actuelle interdisant à l'employeur presque toute surveillance de l'utilisation du téléphone ou de l'ordinateur n'est pas adéquate et ne correspond pas à la réalité. La jurisprudence – qui d'ailleurs n'est pas toujours unanime sur ces questions – et la plupart des juristes s'accordent aujourd'hui sur la légitimité d'une certaine ingérence de l'employeur dans la vie privée des travailleurs, en vue d'assurer une correcte exécution du contrat de travail ou de protéger certains intérêts jugés supérieurs à l'intérêt du travailleur au respect de sa vie privée.

Une convention collective de travail (CCT n° 81) a d'ailleurs confirmé la possibilité d'une "cyber-surveillance", graduelle et sous conditions, des travailleurs. Cette convention collective ne s'applique cependant qu'au secteur privé.

Le contrôle des données de communications électroniques est subordonné au respect par l'employeur des principes de finalité, de proportionnalité et de transparence.

L'employeur se voit reconnaître la possibilité d'exercer un contrôle à la condition que ce contrôle soit effectué pour une ou plusieurs *finalités* considérées comme légitimes. On distingue quatre finalités : 1° la prévention de faits illicites ou diffamatoires, 2° la protection des intérêts commerciaux de l'entreprise, 3° la sécurité et le bon fonctionnement des systèmes informatique de l'entreprise et enfin 4° le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise.

En vertu du principe de *proportionnalité*, ce contrôle doit revêtir, dans toutes les hypothèses, un caractère adéquat, pertinent et non excessif au regard des finalités poursuivies. L'entreprise ne peut faire plus que ce qui est nécessaire au regard des finalités poursuivies.

Le principe de *transparence* est essentiel en ce qu'il impose à l'employeur un devoir préalable d'information sur la politique et les modalités de contrôle de l'entreprise. L'objectif poursuivi est ici de jouer la carte de la prévention et de la clarté. L'information doit être à la fois collective et individuelle : collective via les organes représentatifs mis en place au sein de l'entreprise, individuelle via une mention dans le règlement de travail, le contrat de travail, etc.

Dans le respect des principes évoqués ci-dessus, une procédure d'individualisation des données peut être réalisée seulement en cas d'anomalie préalablement constatée. Cette procédure consiste pour l'employeur à analyser les données globales dont il dispose en vue de retracer l'identité de l'auteur de l'anomalie. En pratique, les éventuelles anomalies peuvent être constatées par la consultation périodique des données de communications électroniques collectées dans l'entreprise (par exemple, en matière d'utilisation d'Internet, en établissant des statistiques relatives aux durées de connexion de façon globale ou service par service ou en recensant les sites les plus visités par les travailleurs). Il s'agit alors pour l'employeur de décortiquer les données en sa possession, comme il le ferait avec les relevés d'une facture téléphonique. Un contrôle ponctuel s'il a lieu est justifié par des indices laissant suspecter une utilisation abusive des outils de travail.

Cette individualisation des données peut se réaliser de manière directe, sans autre formalité, chaque fois que le contrôle s'effectue en raison des trois premières finalités décrites ci-dessus.

Dans les autres cas, l'individualisation des données sera indirecte. Elle sera précédée d'une phase préliminaire de "sonnette d'alarme", visant à informer les travailleurs de l'existence d'une anomalie et à les avertir d'une possible individualisation des données en cas de récidive.

Enfin, vous ne devez pas perdre de vue que la convention collective laisse, en tout état de cause, l'employeur libre de déterminer les modalités d'accès et/ou d'utilisation des outils informatiques de l'entreprise. Autrement dit, l'employeur peut, par exemple, poser certaines conditions à l'usage d'Internet, parmi lesquelles les plus fréquentes sont : l'interdiction d'accéder à des sites de jeux, l'interdiction de participer à des conversations en ligne, le placement de mécanisme de filtrage de certains sites à contenu particulier ou illégal, etc.

78. Puis-je renoncer à mon droit à la vie privée dans le contrat de travail ?

Il arrive que les employeurs tentent de soumettre individuellement aux salariés des engagements écrits équivalant à une abdication complète par les salariés de leur droits.

En fait, sachez que l'abandon de votre droit à la vie privée ne peut intervenir de manière générale et abstraite dans le contrat de travail. Seule une partie de celui-ci pourrait être abandonnée comme le droit de s'opposer à une ingérence dans la vie privée. Une renonciation à un droit fondamental, vu son caractère inaliénable et d'ordre public est soumise à conditions.

Le consentement de l'individu à une telle ingérence doit être individuel, informé, libre, préalable, particulier et révocable. De plus, la renonciation ne peut toucher au noyau dur du droit dont il est question. On peut ainsi dire que si une renonciation à une partie du droit à la vie privée est consentie par l'employé dans le contrat de travail, celle-ci doit, le plus souvent, être confirmée à chaque nouvelle ingérence.

79. Mon employeur peut-il contrôler le contenu de mes e-mails ?

L'utilisation de la messagerie électronique professionnelle pour envoyer ou recevoir, dans des proportions raisonnables, un message à caractère personnel correspond à un usage généralement et socialement admis, mais peut être "réglementé" par l'employeur.

En principe, votre employeur n'est pas autorisé à prendre connaissance du contenu des courriers électroniques émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail. Le courrier électronique est en effet protégé par le secret de la correspondance.

En conséquence, l'ingérence de l'employeur dans la sphère privée du travailleur doit être minimale ; elle doit se limiter au contrôle de l'utilisation de la messagerie électronique et non du contenu des e-mails. On peut affirmer que c'est donc sur base d'une liste des courriers - comme sur base d'une facture de téléphone laissant apparaître des montants anormalement élevés - que l'absence de respect des règles posées par l'employeur pourra être décelée. L'employeur est autorisé à contrôler l'identité du destinataire et de l'auteur, la taille et le type de fichier envoyé, ainsi que le volume des courriers sortants par poste de travail. La prise de connaissance du contenu du courrier électronique est considérée comme excessive, de la même façon que le serait l'écoute ou l'enregistrement de vos communications téléphoniques.

L'employeur peut cependant avoir accès au contenu de vos e-mails dans certaines circonstances. Tel sera le cas notamment si l'employeur obtient votre consentement. Cependant, bien que cela semble controversé, l'employeur doit normalement obtenir le

consentement de tous les participants à la communication, c'est-à-dire aussi celui du destinataire.

80. Mon employeur peut-il surveiller mon utilisation d'Internet ?

La visite d'un site Internet suppose l'établissement d'une connexion entre l'ordinateur au départ duquel le site est visité et un ordinateur distant, sur lequel sont stockées les informations consultées. Cette connexion fait l'objet de données d'identification comparables à celles d'une communication téléphonique : adresse du site, moment et durée de la visite. Ces données sont en outre enregistrées automatiquement sur le serveur de l'entreprise ou celui du fournisseur d'accès d'Internet. Il est dès lors aisé pour l'employeur de vérifier l'utilisation qui est faite d'Internet par ses employés.

Toutefois, le contrôle de l'employeur ne peut entraîner qu'une ingérence minimale dans la vie privée. Un tel contrôle ne peut se faire que dans un nombre limités de cas (*supra*, n° 77).

En outre, ce contrôle, même autorisé, est limité. Il doit porter en premier lieu sur une liste d'adresses de sites consultés de façon globale sur une certaine période et ce n'est que si certaines anomalies sont détectées (durée de visite trop longue, consultation de sites indécents, etc.) que des mesures appropriées peuvent être prises.

Ainsi, un contrôle est possible moyennant d'une part une information préalable, d'autre part le respect des finalités déterminées.

Sachez en outre que les données de trafic entre l'ordinateur que vous utilisez sur votre lieu de travail et un site Internet constituent des données personnelles au sens de la loi sur la protection de la vie privée. Cette loi doit donc être respectée, ce qui signifie notamment que l'employeur doit avertir les travailleurs de la conservation des données de connexion.

CHAPITRE II. LE *SPAMMING*

81. Qu'est-ce que le spamming ?

Au sens large, le terme *spamming* désigne l'envoi, massif et répété, de messages non sollicités, à caractère commercial le plus souvent.

Dans un sens restreint, il vise plus précisément l'envoi de publicités non sollicitées, par courrier électronique, dans un contexte de "collecte sauvage" (entendez : non respectueuse des principes posés par les législations protectrices des données à caractère personnel) des adresses des destinataires.

Or le courrier électronique est, de toute évidence, un vecteur de publicité idéal : pratique, peu onéreux et efficace ! Aussi est-il devenu un instrument très prisé de marketing direct.

82. Comment les annonceurs connaissent-ils mon adresse électronique ?

Les annonceurs obtiennent votre adresse électronique de plusieurs façons :

- Tout d'abord, il est possible que vous ayez communiqué vous-même votre adresse. Ainsi, lorsque vous visitez un site web pour acquérir un produit ou un service, ou lors de votre inscription à une liste de diffusion ou à un forum de discussion, on vous demande souvent d'introduire des données personnelles, telles que vos nom, adresse géographique… et adresse de courrier électronique. Ces données sont souvent réutilisées soit par la personne à laquelle vous les avez fournies, soit par d'autres personnes auxquelles la première personne a transmis ces informations. En outre, certains fournisseurs de messagerie électronique gratuite prévoient qu'en contrepartie vous acceptiez de recevoir des publicités. Diverses offres gratuites d'accès à Internet conditionnent pareillement la gratuité de l'envoi de messages publicitaires par le biais du courrier électronique.

- Ensuite, il existe diverses méthodes de collecte dite "sauvage" réalisée sans ou contre votre consentement : utilisation de logiciels permettant l'inscription à un maximum de listes de diffusion afin de récupérer les adresses électroniques de leurs membres ; collecte automatique d'adresses électroniques dans les espaces publics d'Internet (p. ex. annuaires ou moteurs de recherche, vos pages web personnelles…) ; recours à diverses manœuvres frauduleuses (p. ex. faux concours, offres d'espaces web gratuits…).

- Enfin, il existe un véritable marché des fichiers d'adresses de courrier électronique : des entreprises font leur métier de la mise à disposition (le plus souvent, par le biais d'une location) de tels fichiers. Il est aussi possible de se procurer sur Internet des listes contenant des milliers d'adresses à télécharger pour des sommes relativement modiques.

83. Le spamming m'est-il préjudiciable ?

Vous pouvez effectivement subir deux types de conséquences néfastes :

1. d'une part, si l'envoi est massif, cela peut provoquer un engorgement de votre boîte aux lettres électronique, et donc une difficulté pour accéder au réseau, sans compter les pertes de temps pour lire et supprimer les publicités ;

2. d'autre part, sauf liaison permanente à Internet, vous devez supporter les coûts de connexion nécessaires au téléchargement, qui peuvent être élevés si le message est long à télécharger (parce qu'il contient par exemple un fichier attaché de taille importante).

En outre, la réception de messages peut causer le désagrément lié au fait que certaines publicités peuvent vous paraître agressives ou ne pas correspondre à votre éthique.

84. Les annonceurs ont-ils le droit de m'adresser des e-mails publicitaires non demandés ?

Non ! Selon la loi belge – et bientôt celle de tous les Etats membres de l'Union européenne –, *aucune publicité ne peut vous être envoyée par e-mail sans votre consentement* préalable, libre, spécifique et informé.

Pour le reste, il convient de souligner que les entreprises pratiquant le *marketing* direct par e-mail doivent se conformer en tous points aux principes inscrits dans les législations de protection des données à caractère personnel (*supra*, n^{os} 72 et s.).

Pour rappel, plusieurs droits vous sont reconnus :

- un *droit à l'information* : lorsque vous communiquez des données à caractère personnel à une entreprise via une requête, un bon de commande, un talon d'inscription, un courrier…, elle est tenue de vous préciser à quoi l'information va servir (les finalités du traitement), ainsi que les coordonnées (nom et adresse) du responsable du traitement ;

- un *droit d'accès* : vous pouvez toujours demander à une entreprise quelles données elle détient à votre sujet et elle est tenue de vous répondre dans un délai raisonnable ;

- un *droit de rectification* : vous avez le droit de faire corriger gratuitement les informations inexactes vous concernant.

85. Ai-je le droit de m'opposer à recevoir des e-mails publicitaires ?

Oui ! La loi vous permet de retirer votre consentement à recevoir des publicités par courrier électronique, à tout moment, sans frais, ni indication de motif.

A ce propos, lors de l'envoi de toute publicité par e-mail, l'entreprise qui vous sollicite est tenue :

- de fournir une information claire et compréhensible concernant le droit de vous opposer, pour l'avenir, à recevoir des publicités ;

- d'indiquer et de mettre à votre disposition un moyen approprié d'exercer efficacement ce droit par voie électronique.

86. Que dois-je faire pratiquement pour exercer mon droit d'opposition ?

Deux possibilités s'offrent à vous :

- Si vous ne souhaitez plus recevoir de publicités par e-mail d'une entreprise bien précise, vous pouvez vous adresser à celle-ci et lui demander de supprimer votre adresse e-mail de ses fichiers.

- Si vous souhaitez ne plus recevoir aucune publicité par e-mail d'aucune entreprise, vous pouvez vous inscrire sur la liste Robinson e-mail, gérée par l'Association Belge de Marketing Direct (à cet effet, rendez-vous sur la page http://www.bdma.be, ou directement sur la page http://www.robinsonlist.be/mk/get/ROB_EMAIL). Les données transmises (prénom, nom et adresse e-mail) seront enregistrées dans le fichier Robinson. En principe, vous ne devriez plus recevoir de publicités par e-mail, à tout le moins de la part des nombreuses entreprises affiliées à l'ABMD.

Attention : les entreprises dont vous êtes client ou auxquelles vous avez donné l'autorisation expresse de vous adresser de la publicité par e-mail peuvent continuer à vous envoyer des sollicitations commerciales, en dépit de votre inscription dans la liste Robinson. Si vous souhaitez ne plus recevoir de publicité par e-mail de la part de ces entreprises, vous devez vous adresser à chacune d'entre elles afin de retirer votre consentement à recevoir, dans l'avenir, des publicités par e-mail de leur part.

87. Ces principes valent-ils aussi en matière de SMS ?

Oui ! Les principes exposés plus haut (*supra*, n^{os} 84 et 85) valent également en matière de SMS. En réalité, la loi ne mentionne jamais le terme "*e-mail*", mais celui de "courrier électronique", qui s'entend de manière extrêmement large et englobe indubitablement les SMS.

Sachez que l'ABMD gère également une liste Robinson SMS sur laquelle il vous est possible de vous inscrire pour ne plus recevoir de publicité à votre nom par SMS (à cet effet, rendez-vous sur la page http://www.bdma.beou directement sur la page http://www.robinsonlist.be/mk/get/ROB_SMS).

Cette liste est en tous points comparable à celle existante en matière d'e-mail (*supra*, n° 86).

88. Existe-t-il des moyens techniques pour se protéger du spamming ?

Il existe effectivement divers outils de filtrage permettant de lutter contre le *spamming*. Les filtres sont configurés de manière à isoler les messages indésirables en fonction de divers critères de recherche, notamment l'origine du message (p. ex. l'adresse IP de l'expéditeur) ou son contenu.

A ce propos, il faut savoir que la loi oblige dorénavant l'expéditeur d'un message publicitaire à faire en sorte, d'une part, que le but commercial du message soit identifiable dès sa réception par le destinataire, d'autre part, que la personne physique ou morale pour le compte de laquelle la publicité est faite soit clairement identifiable.

Par ailleurs, lors de l'envoi de publicités par e-mail, il est interdit, d'une part, d'utiliser l'adresse électronique ou l'identité d'un tiers, d'autre part, de falsifier ou de masquer toute

information permettant d'identifier l'origine du message de courrier électronique et son chemin de transmission.

Ces exigences légales devraient faciliter la programmation des filtres selon le critère choisi.

Les filtres programmés en fonction de l'origine des messages permettent de bloquer les publicités en provenance des adresses IP identifiées. Les filtres programmés en fonction du contenu des e-mails permettent, quant à eux, d'éliminer les publicités contenant un mot ou une combinaison de mots précis (p. ex. *sex* ou *make money fast*). Dans ce cas, le risque existe de perdre également des messages sollicités.

Quel que soit le filtre choisi, celui-ci peut être installé soit au niveau du serveur de votre fournisseur d'accès, soit sur votre propre ordinateur.

Le filtrage chez votre fournisseur d'accès constitue la solution la plus commode étant donné qu'il se charge de trier et d'éliminer lui-même les publicités indésirables. Cependant, ce système implique que le processus de tri échappe à votre maîtrise. Or, certains facteurs de sélection (p. ex. la similitude et la quantité de messages envoyés) peuvent conduire au blocage de messages que vous aviez sollicités. De plus, un système de filtrage en fonction du contenu implique un contrôle automatique du contenu de tous les e-mails qui vous sont envoyés, ce qui peut poser des problèmes au regard de la protection de la vie privée.

A l'inverse, lorsque le filtre est placé au niveau de votre ordinateur, les publicités arrivent inévitablement dans votre boîte aux lettres électronique. Par conséquent, vous n'évitez ni le risque d'engorgement, ni l'augmentation de vos coûts de connexion. Si vous disposez d'un logiciel de filtrage, il est sans doute déjà configuré (ainsi, la plupart des logiciels de courrier électronique offrent des possibilités de filtrage). Cependant, vous avez en principe la possibilité de personnaliser le filtre, en ajoutant ou en supprimant des critères de sélection. Le risque de perdre des publicités sollicitées est dès lors moins important puisque vous avez opéré vous-même la sélection. En outre, vos e-mails n'ont pas dû être ouverts par un tiers.

CHAPITRE III. LES CONTENUS ILLICITES ET PREJUDICIABLES

89. Puis-je consulter impunément un contenu illicite sur le net ?

Le seul fait de consulter ou de détenir de l'information constitue rarement un acte illicite. Le motif est simple : lorsqu'une information est problématique, c'est généralement à son auteur que l'on adresse les reproches, et non à celui qui la consulte.

Néanmoins, certaines informations sont à ce point sensibles ou illicites que le législateur a jugé bon de faire peser une partie de responsabilité sur celui qui les lit ou les détient. Les hypothèses visées sont : les secrets d'État et la pédophilie. Seul ce dernier point retient ici l'attention.

Dans la foulée des douloureuses affaires judiciaires qui ont bouleversé la Belgique, la loi du 13 avril 1995 a apporté de nouvelles armes pour lutter contre la pédophilie :

- D'une part, la loi incrimine la seule détention, en connaissance de cause, de photos et autres supports visuels représentant des positions ou des actes sexuels à caractère pornographique impliquant ou présentant des mineurs de moins de 16 ans.

- D'autre part, une nouvelle règle de procédure permet de poursuivre devant les tribunaux répressifs belges, le Belge ou l'étranger trouvé en Belgique qui aurait, dans ou hors du territoire, commis l'infraction reprise ci-dessus, même en l'absence de dénonciation de la part d'une autorité étrangère.

Appliquée à Internet, cette loi ouvre des perspectives inédites : quiconque vit sur le territoire et *détient*, en connaissance de cause, des photos illicites téléchargées à partir du réseau Internet ou qu'il aurait reçues dans un forum de discussion, peut faire l'objet de poursuites en Belgique, même si ces photos sont détenues sur un serveur situé à l'étranger, par exemple sur un des serveurs virtuels proposés sur Internet. Pareillement, l'étranger qui aurait diffusé ces photos, même à partir d'ordinateurs situés à l'étranger, peut être poursuivi en Belgique pour autant qu'il soit *trouvé* en Belgique, par exemple parce qu'il y passe des vacances.

Plusieurs pays ont adopté une législation similaire (France, USA, Canada, etc.).

90. Que faire si je découvre un contenu pédopornographique sur le net ?

Il faut bien entendu éviter de consulter des informations pouvant revêtir un caractère pédophile (une directive ministérielle en vigueur depuis le 1er sept. 1999 décrit la pédopornographie comme "des objets ou supports visuels de toute nature qui représentent des positions ou des actes sexuels à caractère pornographique, impliquant ou représentant des mineurs d'âge").

Si certains fichiers ont été téléchargés indépendamment de votre volonté, il est inutile de paniquer : il suffit le plus souvent de les effacer et de ne plus consulter le service sur lequel ils ont été trouvés.

Vous pouvez aussi aller plus loin et dénoncer ce service. Plusieurs possibilités s'offrent à vous :

1. Vous pouvez envoyer un courrier, téléphoner ou vous rendre à n'importe quel commissariat de police.

2. Vous pouvez aussi agir, par voie électronique, conformément à la procédure mise en place dans le cadre de l'accord conclu entre l'Association des Fournisseurs d'Accès à Internet (ISPA) et les ministères de la Justice et des Télécommunications :

   - Tout le monde peut dénoncer un contenu qu'il estime illicite auprès de son fournisseur d'accès ou au point de contact de la police judiciaire (e-mail : contact@gpj.be). Si la dénonciation est faite au fournisseur, celui-ci la transmet lui-même au point de contact.

   - Le point de contact fait un tri. S'il estime que l'information n'est *manifestement pas* illicite, le dossier est classé. Dans les autres cas, le dossier est transmis au parquet. Simultanément, l'ISPA est avertie et ses membres s'engagent à bloquer l'accès au contenu par tous les moyens dont ils peuvent raisonnablement disposer.

   - Toute information complémentaire peut être obtenue sur le site de l'ISPA (http://www.ispa.be) ou sur le site de la police judiciaire (http://www.gpj.be).

3. Enfin, vous pouvez vous adresser à *Child Focus*, soit par téléphone (en appelant le 110), soit via son site web (www.childfocus-net-alert.be) :

   - www.childfocus-net-alert.be préserve votre anonymat dès l'instant où vous en exprimez le souhait. Le serveur est configuré de manière à ce qu'il soit impossible d'analyser l'identité des personnes qui transmettent des informations ou qui visitent le site sur la base des données log puisque celles-ci ne sont pas conservées.

   - De plus, le serveur web est également configuré de manière à ce que le visiteur n'ait pas de '*cookie*' après avoir visité le site (*supra*, n° 64).

   - Enfin, vous bénéficiez d'une communication sécurisée : le serveur web reçoit les données telles qu'encodées par vous et, si vous ne communiquez pas de données personnelles, il n'enregistre aucune information vous concernant.

91. Comment protéger les mineurs contre des contenus indésirables ?

Internet recèle des contenus que vous jugez inappropriés pour des mineurs qui bénéficient d'un accès à Internet dans une bibliothèque, à l'école ou dans le cadre familial. L'on songe notamment aux sites à contenu violent, pornographique, haineux ou raciste, aux sites des sectes ou à ceux qui font du commerce de drogues. En tant qu'éducateur, responsable de jeunes ou parent, vous souhaitez mettre ces mineurs à l'abri de tels contenus indésirables ou préjudiciables. C'est possible grâce à des systèmes d'évaluation et de filtrage disponibles sur le marché.

Un système de filtrage se compose d'un ou plusieurs logiciels visant à empêcher les utilisateurs d'Internet d'accéder à certains contenus. Un tel système repose sur deux composants : l'évaluation et le filtrage.

L'évaluation consiste à procéder à un classement des sites web selon leur contenu en appliquant des jugements de valeur.

Le logiciel de filtrage examine quant à lui la ressource à laquelle l'utilisateur souhaite accéder. Si cette ressource ne correspond pas aux critères autorisés pour y accéder, le logiciel annonce à l'utilisateur que l'accès à cette ressource est refusé et le navigateur web n'affiche pas le contenu de ce site.

92. Quels sont les systèmes de filtrage disponibles ?

Les outils de filtrage autonomes utilisent une combinaison de deux approches pour évaluer le contenu : l'établissement d'une liste de sites acceptables ou inacceptables et une sélection par mots-clés.

Le blocage basé sur des listes s'appuie sur une énumération explicite des sites qui doivent être autorisés (listes blanches) ou interdits (listes noires). Ces listes sont généralement constituées par les vendeurs du logiciel selon leurs critères propres.

Par ailleurs, le consortium W3 a développé un standard ouvert appelé PICS (*Platform for Internet Content Selection*). Il s'agit d'un protocole d'échange de données d'évaluation. Le but est de mettre un outil à disposition des internautes pour leur permettre de sélectionner le contenu selon leurs propres critères éthiques.

En pratique, vous pouvez sélectionner un système d'évaluation correspondant à vos valeurs. Les systèmes aujourd'hui les plus connus sont ceux de RSACi, de SafeSurf et de Netshepherd.

93. Les systèmes de filtrage sont-ils efficaces ?

La valeur et l'efficacité des systèmes fondés sur des listes dépendent des choix effectués par les vendeurs. A cet égard, la marge de manœuvre est faible, voire inexistante. De plus, la liste devient vite obsolète, à mesure de l'apparition de nouveaux sites. Quant à la sélection par mots-clés, elle a ses limites car elle ne tient pas compte du contexte et aboutit souvent à bloquer des sites sans raison valable.

Quant au système PICS, il laisse davantage de choix aux parents, mais les systèmes d'évaluation sont encore peu nombreux. Par ailleurs et surtout, le succès de cette initiative requiert l'évaluation d'un pourcentage significatif des sites web. Force est de constater que la masse critique des sites évalués est encore faible actuellement.

94. Que faire si je découvre sur le net un contenu illicite ou préjudiciable ?

Comment réagir si vous vous estimez agressé ou préjudicié par un contenu illicite (violent, révisionniste, pédophile, raciste…) ou par un contenu diffamatoire à votre égard ou portant atteinte à votre honneur, à votre réputation, à votre vie privée…?

Tout d'abord, vous pouvez vous adresser à votre fournisseur d'accès ou à l'hébergeur du site concerné (ou du groupe de discussion…), pour attirer son attention sur le contenu préjudiciable et lui demander, selon le cas, de bloquer l'accès à ce dernier ou de le supprimer. Vous avez intérêt à conserver trace de votre requête.

En cas d'absence de réaction, vous pouvez porter plainte auprès du commissariat de police le plus proche. Cette plainte sera transmise aux autorités judiciaires compétentes qui pourront ouvrir une instruction et entamer, le cas échéant, des poursuites devant une juridiction répressive.

Si vous estimez avoir subi un dommage personnel – matériel (p. ex. perte de clients suite à la diffusion d'informations diffamatoires ou calomnieuses à votre égard) ou moral (p. ex. atteinte à votre honneur ou à l'intimité de votre vie privée) –, sachez qu'il vous est possible de réclamer une indemnisation. A cet effet, il est conseillé d'introduire votre plainte avec constitution de partie civile.

Indépendamment de toutes poursuites judiciaires, il vous est également loisible de demander réparation du dommage subi, en introduisant une action en responsabilité civile auprès d'un tribunal civil.

Si vous souhaitez qu'il soit mis fin, au plus vite, à la diffusion du contenu que vous jugez attentatoire à vos droits, sachez qu'il existe des procédures rapides vous permettant d'obtenir une décision satisfaisante dans un délai de 24 h. à quelques jours. Si vous avez gain de cause, le juge pourrait ordonner, par exemple, le blocage de l'accès au contenu litigieux ou le retrait immédiat de celui-ci.

95. Qui puis-je assigner en justice pour obtenir réparation du dommage subi ?

Sachez que la loi prévoit des exemptions de responsabilité au profit de diverses activités intermédiaires sur Internet. Ainsi, l'activité de simple transmission et celle de fourniture d'accès à Internet bénéficient d'une immunité presque totale à l'égard des contenus véhiculés. Vous aurez donc rarement intérêt à traduire en justice l'opérateur de réseau ou le fournisseur d'accès que vous jugez responsable de votre préjudice.

Vous aurez plus de chances de succès si vous décidez de traduire en justice l'hébergeur du contenu litigieux (pourvu que vous le connaissiez). Néanmoins, la loi prévoit également une limitation de responsabilité au profit de l'activité d'hébergement. Ainsi, la responsabilité de l'hébergeur ne pourra pas être engagée s'il n'avait pas connaissance du contenu illicite ou s'il a agi promptement, dès le moment où il a été averti de la présence du contenu illicite, pour le retirer ou rendre l'accès à celui-ci impossible.

En toute hypothèse, vous avez donc intérêt à mettre en cause la responsabilité de l'auteur de l'information litigieuse, pour autant bien entendu que vous ayez pu l'identifier.

CHAPITRE IV. LA CYBERCRIMINALITE

Section 1. Le faux en informatique

96. Qu'est-ce qu'un faux en informatique ?

Selon la loi, commet un "faux en informatique" celui qui introduit dans un système informatique, modifie ou efface des données, qui sont stockées, traitées ou transmises par un système informatique, ou modifie par tout moyen technologique l'utilisation possible des données dans un système informatique, et par là, modifie la portée juridique de telles données.

En clair, le faux en informatique vise la dissimulation intentionnelle de la vérité par le biais de manipulations informatiques de données pertinentes sur le plan juridique. Des données électroniques peuvent être ainsi falsifiées moyennant modification ou effacement (complet ou partiel) lors de leur saisie (introduction dans l'ordinateur), de leur récupération ou au cours de leur stockage.

Si, pour falsifier des données, vous vous êtes introduit sans autorisation dans un système informatique, il se peut que vous vous soyez également rendu coupable de *hacking* (*infra*, n^{os} 104 et s.). Voire aussi de fraude informatique si l'opération vous a procuré un avantage patrimonial (*infra*, n^{os} 100 et s.). Dans ce cas dit "de concours idéal d'infractions", la peine la plus forte sera seule prononcée.

97. Quels sont les exemples de faux en informatique ?

Constituent des faux en informatique, notamment : la confection illégale ou la falsification de cartes de crédit ; les faux en matière de contrats numériques (lorsque les données juridiquement pertinentes ne sont plus imprimées sur papier, ni signées à l'aide de la main) ; l'introduction d'un faux numéro de carte de crédit lors de l'inscription à un site Internet payant ; l'inscription de créances fictives ou la modification de données salariales par un employé dans le logiciel comptable de l'entreprise ; le fait, pour un employé, de gonfler artificiellement les heures supplémentaires encodées dans le logiciel de gestion du temps de travail ; la falsification d'une signature électronique ou encore l'utilisation en pleine connaissance de cause de données falsifiées.

98. Le faux en informatique est-il punissable pénalement ?

Celui qui commet un faux en informatique est puni d'un emprisonnement de six mois à cinq ans et d'une peine d'amende ou d'une de ces peines seulement. La tentative de commettre un faux est également punie. En cas de récidive, les peines prévues sont doublées.

99. Puis-je commettre un faux en informatique "sans en être conscient" ?

Non ! Pour être punissable, le faux en informatique doit être commis en connaissance de cause et avec une intention frauduleuse ou à dessein de nuire.

En résumé, l'infraction sera établie si et seulement si tous ses éléments constitutifs sont réunis, à savoir :

- Il faut qu'il y ait introduction, modification ou effacement de données dans un système informatique ou encore modification possible de l'utilisation de ces données.

- Il est nécessaire que cette manipulation entraîne une modification de la portée juridique des données falsifiées.

- L'auteur du faux doit être animé d'une intention frauduleuse ou agir dans le but de nuire.

Section 2. La fraude informatique

100. Qu'est-ce que la fraude informatique ?

Selon la loi, se rend coupable de "fraude informatique" celui qui se procure, pour soi-même ou pour autrui, un avantage patrimonial en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique.

En clair, la fraude informatique vise celui qui se procure un avantage patrimonial frauduleux par le biais d'une manipulation illicite de données électroniques.

101. Quels sont les exemples de fraude informatique ?

La fraude informatique peut viser l'utilisation d'une carte de crédit volée pour retirer de l'argent d'un distributeur automatique de billets, le dépassement illicite du crédit octroyé par sa propre carte de crédit, l'introduction d'instructions de programmation permettant d'obtenir à la suite de certaines transactions d'autres résultats en vue d'un avantage financier illicite, ou encore les manipulations illégitimes effectuées par un employé de banque sur les comptes des clients.

102. La fraude informatique est-elle punissable pénalement ?

L'auteur d'une fraude informatique est puni d'un emprisonnement de six mois à cinq ans et d'une amende ou d'une de ces peines seulement. La tentative de fraude est également punie. En cas de récidive, les peines prévues sont doublées.

103. Puis-je commettre une fraude informatique "sans en être conscient" ?

Non ! Pour être punissable, la fraude informatique exige une intention frauduleuse. A la différence de l'escroquerie, il n'est pas question ici de manipulation directement destinée à tromper la confiance d'une personne. Il faut, mais il suffit, que soit établie l'intention de se procurer ou de procurer à autrui un avantage patrimonial illicite.

Section 3. Le hacking

104. Qu'est-ce que le hacking ?

Selon la loi, celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et d'une amende ou d'une de ces peines seulement. Par ailleurs, celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende ou d'une de ces peines seulement.

La tentative de commettre l'une de ces infractions est punie des mêmes peines que l'infraction elle-même. En cas de récidive, les peines prévues sont doublées.

En clair, la loi distingue deux hypothèses : l'accès non autorisé au système informatique d'un tiers ou le fait de s'y maintenir (*hacking* externe), d'une part, le fait d'outrepasser son pouvoir d'accès à ce système (*hacking* interne), d'autre part.

Dans le premier cas, il suffit que l'auteur agisse en pleine connaissance des éléments de l'acte posé et en voulant ou, du moins, en acceptant leur réalisation. En d'autres termes, l'infraction de *hacking* externe n'exige nullement que l'accès non autorisé au système ou le fait de s'y maintenir soit inspiré par une intention frauduleuse ou réalisé dans le but de nuire (*supra*, n° 103). Si l'infraction est commise avec une telle intention ou un tel objectif, la peine s'en trouvera seulement aggravée (*infra*, n° 106). L'élément de maintien dans le système informatique est présent dès l'instant où l'intrus s'y "promène" un certain temps, et ce, quand bien même l'accès au système n'aurait pas été commis de manière illicite. C'est dire le caractère large de l'infraction !

Dans le second cas, il faut que l'auteur, qui jouit de droits d'accès à un système mais outrepasse ceux-ci, agisse avec une intention frauduleuse (c'est-à-dire en vue de se procurer un profit ou un avantage illicite) ou dans le but de nuire. En d'autres termes, le *hacking* interne – réalisé, par un employé, un ouvrier, un fonctionnaire ou un consultant indépendant, depuis l'intérieur d'une entreprise, d'une institution, d'une administration ou d'une organisation – n'est punissable que si le sujet indélicat (p. ex. l'employé trop curieux qui va lire des dossiers confidentiels, dont il n'est pas censé pouvoir prendre connaissance) est animé d'une intention particulière comme l'appât du gain illicite ou la malveillance. L'abus du pouvoir d'accès à un système peut prendre diverses formes : soit une personne dispose d'un pouvoir d'accès limité et s'introduit dans des parties du système auxquelles elle n'est pas autorisée à accéder, soit elle dispose de pouvoirs limités à l'égard des données et effectue des manipulations non autorisées (p. ex. elle modifie ou supprime des données qui lui sont accessibles en simple lecture).

105. L'accès non autorisé par jeu, par défi ou pour tester la sécurité d'un système est-il punissable ?

Il n'est permis, en aucun cas, de pénétrer sans autorisation dans le système informatique d'un tiers, ni pour satisfaire une simple curiosité, ni par jeu ou défi, ni pour vérifier l'aptitude du système à résister aux intrusions ou "attaques" extérieures.

L'intrusion ludique par de jeunes fous de l'informatique ou celle, expérimentale et désintéressée, de "chevaliers blancs" est punissable au même titre que l'accès non autorisé dans un système aux fins d'espionnage industriel à but lucratif ou militaire.

La loi pénalise ainsi le simple accès non autorisé à un système ou le maintien dans le système, sans poser d'autres conditions telles que le fait d'avoir "craqué" un dispositif de sécurité, l'intention de se procurer des données ou la volonté d'effectuer un sabotage (destruction de données…).

Néanmoins, pour échapper aux poursuites, le "*hacker*" pourra tenter d'invoquer sa bonne foi, en faisant valoir qu'il ignorait l'interdiction d'accès ou n'avait pas la volonté de passer outre cette interdiction. Il est évident, toutefois, que sa bonne foi sera peu crédible et l'échappatoire difficilement admise s'il a dérobé un code d'accès ou s'il est passé outre un message d'avertissement dissuasif.

106. Existe-t-il des circonstances aggravantes susceptibles d'alourdir la peine ?

La loi prévoit des circonstances aggravantes et un alourdissement de la peine lorsque celui qui accède sans autorisation à un système informatique, tant depuis l'extérieur que de l'intérieur, adopte l'un des comportements suivants :

- reprendre, de quelque manière que ce soit, les données stockées, traitées ou transmises par le système informatique. Est ainsi visé, par exemple, le vol de secrets d'entreprise dans le cadre de l'espionnage industriel ; ou

- faire un usage quelconque d'un système informatique appartenant à un tiers ou se servir du système informatique pour accéder au système informatique d'un tiers. On vise ici, par exemple, l'utilisation de la capacité du système, entraînant une limitation temporaire des possibilités d'autres utilisateurs ou l'utilisation du système comme "tremplin" (relais) pour accéder de façon détournée à un autre système ; ou

- causer un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui sont stockées, traitées ou transmises par ce système ou au système informatique d'un tiers ou aux données qui sont stockées, traitées ou transmises par ce système.

Sont également punissables celui qui ordonne ou stimule des actes de *hacking* et celui qui recèle, divulgue ou fait un usage quelconque des données obtenues suite à la commission de faits de *hacking*.

107. Puis-je être victime de hacking ? Comment m'en protéger ?

Évidemment ! Certains surfeurs sur Internet sont passés maîtres dans l'art de pénétrer les systèmes informatiques connectés au réseau, parfois par jeu, pour relever un défi ou, tout simplement, pour nuire ou semer la pagaille. Il serait naïf de vous croire à l'abri de pareils agissements, sous prétexte que vous n'avez rien à vous reprocher ou que votre système ne contient rien de bien extraordinaire.

Pour vous protéger, le mieux est d'installer un *firewall* (pare-feu), c'est-à-dire un dispositif, logiciel ou matériel, destiné précisément à dresser un mur de sécurité entre votre système et le reste du réseau, de manière à empêcher toute intrusion non autorisée dans votre système de la part des tiers.

Un *firewall* ne vous indiquera toutefois pas toujours les éventuelles intrusions dont votre système aurait fait l'objet. C'est la raison pour laquelle l'élaboration d'un système de sécurité efficace passe le plus souvent par l'adjonction au système informatique d'un dispositif de détection des intrusions (I.D.S., pour *Intrusion Detection System*).

Section 4. L'envoi / la réception de virus

108. Qu'est-ce qu'un virus informatique ?

Un virus est un programme destiné à perturber le fonctionnement des systèmes informatiques, ou pire, à modifier, corrompre, voire détruire, les données qui y sont stockées.

Capable de se reproduire de lui-même, le virus est conçu pour détecter d'autres programmes et les infecter en leur incorporant sa propre copie. L'activation du virus

s'opère au moment où le programme infecté est exécuté. Une fois activé, le virus commence à produire ses effets, qui peuvent s'avérer simplement gênants ou incommodants, mais aussi désastreux, voire franchement catastrophiques.

Sont ainsi contrariants, mais d'ordinaire inoffensifs, les virus qui ont pour conséquence d'intervertir certaines lettres du clavier ou qui commandent au disque dur d'afficher un message déterminé à une heure précise.

Nettement plus pernicieux sont les virus qui ont un potentiel de destruction, par exemple, en désordonnant les données contenues dans vos documents ou – pire – en reformatant votre disque dur.

D'autres virus n'ont pas pour effet de détruire spécifiquement vos données, mais constituent néanmoins une menace importante. Par exemple, en colonisant votre espace disque et votre mémoire vive, ils engendrent des baisses de performances significatives.

Enfin, les virus peuvent être à l'origine de véritables catastrophes sur le plan économique ou humain. L'on songe à la paralysie d'un réseau hospitalier ou aux dysfonctionnements occasionnés au système informatique d'un aéroport par des cyber-terroristes.

Étant donné la redoutable capacité des virus à se reproduire, plus la parade sera lente à venir, plus votre ordinateur régressera en termes de performances et/ou plus les dégâts seront importants.

109. Quel est le cycle d'un virus informatique ?

Les virus informatiques, tout comme les virus biologiques, possèdent un cycle de vie, qui va de la création à l'éradication :

Création : c'est la période qu'un programmeur consacre à développer un virus, qu'il soit féroce ou non.

Gestation : c'est la période pendant laquelle le virus est copié en un endroit stratégique afin que sa diffusion soit la plus rapide possible. Le virus infecte en général un programme très populaire et se transmet par l'intermédiaire des *attachements* liés au courrier électronique, d'Internet ou au sein d'une entreprise, d'une école, etc.

Reproduction : les virus, par leur nature, cherchent à se reproduire. Un virus correctement conçu se reproduira un nombre de fois important avant de s'activer. C'est là le meilleur moyen d'assurer la pérennité d'un virus.

Activation : certains virus ne s'activent que lorsque certaines conditions sont réunies. Ils s'activent à certaines dates ou possèdent un système de compte à rebours interne. D'autres ne nécessitent pas de procédure d'activation spécifique et peuvent causer des dommages à votre système en s'appropriant petit à petit l'ensemble de vos ressources.

Découverte : la découverte d'un virus est le moment où quelqu'un se rend compte de sa présence et parvient à l'isoler. Une fois cette opération réalisée, le nouveau virus est généralement transmis au NCSA (*National Computer Security Association*) à Washington DC où il est documenté puis distribué aux développeurs de logiciels antivirus.

Assimilation : une fois la découverte faite, les développeurs d'antivirus modifient leurs programmes pour qu'ils puissent détecter la présence du virus. Cette phase dure entre un jour et six mois.

Éradication : si un nombre suffisant de développeurs d'antivirus sont capables de faire face au virus et si suffisamment de personnes se procurent l'antivirus adéquat, il est possible d'annihiler un virus ou en tout cas de réduire la menace.

110. Comment contracte-t-on un virus ?

Les virus se reproduisent sur le code des autres programmes. Ils sont donc inoffensifs tant que vous n'exécutez pas le programme infecté. En d'autres mots, télécharger un programme infecté d'un site Web ou insérer une disquette dans votre ordinateur est généralement inoffensif, *jusqu'à ce que vous démarriez un logiciel ou que vous ouvriez un fichier !*

Une fois qu'une application ou qu'un fichier infecté est lancé, le virus peut se propager sur d'autres applications et d'autres fichiers. Dans ces conditions, les logiciels ou fichiers que vous partagez avec des amis ou collègues de travail, via une disquette, Internet ou un réseau local, peuvent aussi être infectés, et vous pouvez dès lors transmettre le virus à d'autres ordinateurs.

Il n'est pas possible d'être infecté par un virus simplement en lisant un e-mail au format texte. Le format texte est incapable de contenir un virus. En revanche, il est tout à fait possible de transmettre un virus sous la forme d'une pièce jointe à un message électronique (attachement). Les virus macro, qui sont les plus répandus à l'heure actuelle, sont transmis essentiellement au sein de fichiers de type Word joints à des e-mails. Cependant, les e-mail transmis en HTML sont potentiellement la cible de virus.

Sachez néanmoins que, depuis peu, certaines versions de logiciels de courrier électronique, comme Outlook Express et Netscape Messenger, permettent l'exécution de "scripts" par la simple lecture de l'e-mail. Ces petits programmes peuvent donc infecter votre ordinateur à la simple lecture d'un e-mail. Ceci ne vous arrivera pas en utilisant le logiciel Eudora par exemple.

111. Comment savoir si mon ordinateur est contaminé ?

Les virus sont souvent repérés trop tard par les conséquences désastreuses de leur activité : affichage de messages intempestifs, émission de sons ou de musiques inattendus, mais aussi blocage de l'ordinateur, formatage du disque dur, …

Pourtant, de nombreux indices peuvent vous mettre la puce à l'oreille. Il peut s'agir d'une "mémoire système" disponible inférieure à ce qu'elle devrait être, d'un changement du nom de volume d'un disque, de programmes ou de fichiers subitement absents, de l'apparition de programmes ou de fichiers inconnus ou encore du comportement anormal de certains programmes ou fichiers.

Vous pouvez également utiliser le service gratuit *HouseCall* de l'éditeur Trend pour procéder immédiatement à l'analyse ainsi qu'à l'éradication de virus éventuellement présents sur vos disques (http://news.secuser.com/index.htm).

112. Comment se prémunir contre les virus ?

Bien qu'elle ne vous mette pas à l'abri de tout danger, la meilleure protection consiste à installer sur votre ordinateur un logiciel antivirus. La plupart de ces logiciels proposent une procédure permettant de désinfecter le contenu du disque avant d'installer le logiciel, mais le mieux est d'installer l'antivirus avant toute contamination afin de bénéficier de l'ensemble

de ses fonctionnalités (surveillance des transferts de fichiers ou de l'accès aux fichiers sensibles, inoculation des fichiers pour repérer tout changement de taille suspect, etc.).

Cependant, de nouveaux virus apparaissent chaque jour. Il importe donc d'actualiser régulièrement le logiciel antivirus : la plupart des éditeurs proposent une mise à jour au minimum mensuelle, mais pas toujours gratuite...

Face à cette incertitude, des règles fondamentales s'imposent : la prévention est toujours payante.

- Ne téléchargez pas des programmes d'origine douteuse, qui peuvent vous être proposés sur des sites ou des "*chats*" suspects ;

- Méfiez-vous de certains fichiers joints aux messages que vous recevez : préférez détruire un mail douteux (expéditeur inconnu, etc.), plutôt que d'infecter votre machine ;

- Fuyez les disquettes d'origine suspecte (ou ayant transité dans des lieux publics vulnérables comme les salles des écoles ou universités). Lorsque vous vous rendez dans ces salles informatiques à grande fréquentation, protégez vos disquettes en écriture (le petit verrou dans le coin inférieur droit de votre disquette doit être actionné de telle manière que l'on voie à travers) ;

- Procédez régulièrement à des sauvegardes du contenu important de votre disque dur après avoir vérifié l'absence de virus : cela peut paraître fastidieux, mais en cas d'infection (ou même simplement en cas de crash du disque dur), cela vous sauvera la mise... ;

- Tenez-vous au courant des apparitions de nouveaux virus. Certains magazines vous offrent gratuitement ce service en émettant des "alertes contamination" lorsqu'un virus connaît une diffusion importante. C'est le cas notamment du magazine *Secuser News* : http://news.secuser.com/index.htm.

113. L'envoi d'un virus est-il pénalement sanctionné ?

La loi réprime effectivement la conception, la mise à disposition, la diffusion ou la commercialisation de virus ou de programmes permettant de créer pareils virus.

L'auteur d'une telle infraction est puni d'un emprisonnement de six mois à trois ans et d'une amende ou d'une de ces peines seulement.

En cas de récidive, les peines prévues sont doublées.

114. Puis-je envoyer un virus “sympathique” par jeu ou par blague ?

De nombreux internautes s’envoient de petits programmes amusants, destinés à faire apparaître automatiquement des animations, du texte, des images, du son ou de la vidéo, sur l’ordinateur de celui qui les ouvre, contre sa volonté. Il s’agit également d’une forme de virus, parfois inoffensive, mais parfois susceptible de perturber gravement le fonctionnement d’un système informatique. Dès lors, mieux vaut être prudent avant d’ouvrir ou de faire suivre de tels fichiers, si sympathiques soient-ils.

En principe, seul peut être poursuivi et se voir éventuellement infliger une peine celui qui, avec une intention frauduleuse ou dans le but de nuire, envoie un virus. Il faut donc savoir que le message envoyé est susceptible de causer des dommages (empêcher, totalement ou partiellement, le fonctionnement correct du système informatique de la “victime”).

115. Puis-je être pénalement sanctionné si je propage, à mon insu, un virus venu infecter mon carnet d’adresses ?

Non ! Pour être punissable, il faut être conscient que le virus diffusé est susceptible d’endommager des données ou d’entraver l’utilisation d’un système informatique et vouloir, ou du moins accepter, la réalisation de ces effets.

Par conséquent, n’est pas punissable l’usager qui propage un virus à son insu, ayant lui-même reçu le virus avec son cortège de vicissitudes : carnet d’adresses infecté, apparition de nouveaux fichiers... et envoi non voulu d’e-mails à divers correspondants non sélectionnés...

116. Que penser des e-mails qui m’avertissent qu’un dangereux virus est en circulation ?

Dans la plupart des cas, ces messages catastrophistes sont envoyés par de mauvais plaisantins et ensuite relayés par d’autres usagers, souvent de bonne foi. Ceci dit, on n’est jamais trop prudent et le mieux est de s’informer auprès d’une personne autorisée.

Plusieurs sites proposent une liste régulièrement mise à jour des différents canulars (*hoax*) circulant sur le *net* (*supra*, n° 26).

Section 5. D’autres questions que vous vous posez

117. Les autorités judiciaires ou policières peuvent-elles débarquer chez moi et saisir mon matériel informatique ?

Si vous êtes soupçonné d’actes de piratage, d’accès irréguliers à des systèmes informatiques, d’actes de contrefaçon (reproductions d’œuvres protégées par des droits d’auteur) ou d’autres délits encore (détention d’images pédophiles, communications à caractère raciste ou révisionniste…), les autorités judiciaires et policières peuvent effectivement se présenter chez vous et saisir votre disque dur, vos disquettes, voire tout votre matériel informatique pourvu qu’elles soient munies d’un mandat de perquisition.

118. Peuvent-elles copier des données stockées sur mon disque dur (ou sur des supports mobiles m'appartenant) ?

Effectivement, lorsque la saisie du matériel et des supports informatiques n'est pas souhaitable, les données litigieuses peuvent être simplement copiées, en principe sur des supports appartenant à l'autorité.

Néanmoins, en cas d'urgence ou pour des raisons techniques (le volume des données excède les capacités de stockage des supports amenés par l'autorité), elles peuvent être copiées sur des supports vous appartenant. Peuvent également être copiés les logiciels ayant servi à la création des données, ainsi que les clés permettant de les déchiffrer.

119. Peuvent-elles m'empêcher d'accéder à certaines données ou les éliminer ?

Oui ! Le Procureur du Roi peut empêcher l'accès aux données ayant fait l'objet de copies (notamment par le biais de leur chiffrement, c'est-à-dire en les transformant, à l'aide d'un cryptosystème, en une chaîne de caractères alphanumériques incompréhensibles pour le commun des mortels).

Le but de l'opération est de vous priver de la maîtrise des données "saisies" et d'éviter que l'original des données soit altéré et ne puisse plus servir comme preuve en justice.

Le blocage d'accès peut également remplacer la copie des données lorsque celle-ci s'avère impossible (pour des raisons techniques ou à cause du volume des données).

En principe, les données ne peuvent jamais être purement et simplement détruites en dehors d'un jugement. A titre d'exception, la loi permet la destruction de certains types de données, à savoir celles manifestement contraires à l'ordre public ou aux bonnes mœurs : images pédophiles, virus particulièrement pernicieux...

120. Peuvent-elles m'obliger à leur fournir des informations sur la manière d'accéder à certaines données protégées ?

Les autorités chargées d'enquêtes peuvent requérir la collaboration des personnes disposant des clés d'accès au système informatique et aux données y stockées. Elles peuvent ordonner à toutes les personnes susceptibles de connaître votre système informatique de fournir des informations sur le fonctionnement du système et sur la manière d'y accéder ou d'accéder aux données. Ainsi, elles pourront demander leur collaboration pour faire sauter des protections ou déchiffrer des données codées.

Le juge d'instruction peut aussi ordonner à toute personne appropriée de mettre en fonctionnement elle-même le système informatique ou, selon le cas, de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les informations pertinentes qui sont stockées, traitées ou transmises par le système.

Toutefois, si vous êtes inculpé, vous n'êtes pas tenu d'obéir à cet ordre, pas plus que vos proches. Il s'agit là d'un principe fondamental : toute personne accusée d'une infraction bénéficie d'un droit au silence qui l'autorise à se taire et à ne pas communiquer une information susceptible de l'incriminer.

Peuvent être ainsi tenus de prêter leur concours non seulement le responsable du système ou d'autres utilisateurs, mais aussi le gestionnaire du réseau, le concepteur ou le fournisseur du logiciel de décryptage, des tiers de confiance (par exemple, un prestataire de services de certification), voire des experts en sécurité informatique qui maîtriseraient le cryptosystème sécurisant les données litigieuses.

Le refus de collaboration ou le fait de faire obstacle à la recherche dans un système informatique peut être sanctionné d'un emprisonnement de six mois à un an et d'une amende ou d'une de ces peines seulement.

121. En tant qu'utilisateur d'Internet, mes données d'appel et d'identification sont-elles enregistrées et conservées par certains opérateurs de réseaux et de services ?

Oui ! La loi impose aux opérateurs de réseaux téléphoniques ou mobilophoniques, aux fournisseurs d'accès à Internet, de courriers électroniques, de services *chat*, de forums de discussion, etc., d'enregistrer et de conserver vos données d'appel et d'identification pour une durée ne pouvant être inférieure à douze mois.

Cette obligation de conservation (*ex ante*, ou préalable) est permanente, et non liée à une procédure d'enquête en cours (information ou instruction).

La loi ne définit pas ce qu'elle entend par "données", ni les types de données concernées par l'obligation de conservation, pas plus qu'elle ne détermine les prestataires visés par cette obligation. Les données d'appel et d'identification peuvent inclure, semble-t-il, les heures et durée de connexion, la provenance des appels, l'adresse IP de votre machine…

Cette obligation, large et imprécise, est prévue en vue de faciliter la recherche et la poursuite d'infractions pénales. Un arrêté royal devrait déterminer la liste des données concernées. Cette solution est critiquable dans la mesure où la Constitution prévoit que les restrictions à la vie privée doivent être permises par une loi.

Partie 5.
Contracter sur le *net*

CHAPITRE I. LES INFORMATIONS

En vertu de la loi, le prestataire est tenu de faire figurer sur son site web un certain nombre d'informations, relatives à son activité, aux modalités du contrat, aux produits et aux services offerts, à votre commande, etc.

122. A qui ai-je affaire ? Quels renseignements suis-je en droit de trouver concernant le prestataire et ses activités ?

Afin de garantir une certaine transparence dans les relations contractuelles qui se nouent sur les réseaux, le prestataire doit fournir à tous ses visiteurs un minimum d'informations concernant son activité, à savoir :

- son nom ou sa dénomination sociale ;
- l'adresse géographique où il est établi ;
- ses coordonnées, y compris son adresse de courrier électronique, permettant d'entrer en contact rapidement et de communiquer directement et efficacement avec lui ;
- le cas échéant, le registre de commerce auprès duquel il est inscrit et son numéro d'immatriculation ;
- le cas échéant, son numéro de TVA ;
- les codes de conduite auxquels il est éventuellement soumis ainsi que les informations relatives à la façon dont ces codes peuvent être consultés par voie électronique (*infra*, n^{os} 179 et s.) ;
- dans le cas où l'activité du prestataire est soumise à un régime d'autorisation, les coordonnées de l'autorité de surveillance compétente ;
- et enfin, pour les prestataires exerçant une profession réglementée (p. ex. les professions libérales) :
  - l'association professionnelle ou l'organisation professionnelle auprès de laquelle le prestataire est inscrit,
  - le titre professionnel et l'État dans lequel il a été octroyé,
  - une référence aux règles professionnelles applicables et aux moyens d'y avoir accès.

Ces informations doivent être disponibles en toute hypothèse, qu'il s'agisse d'un site de commerce électronique, d'un site d'information, d'un moteur de recherche, d'un fournisseur d'accès à Internet, d'un fournisseur de messagerie, d'un forum de discussion, etc.

L'accès à ces informations doit être facile, direct et permanent, par exemple en cliquant sur un hyperlien placé en bas de chaque page web, renvoyant à une page spécifique contenant ces informations.

123. Comment distinguer une publicité d'une autre information sur les réseaux ?

Il vous est sans doute déjà arrivé de vous faire "piéger" sur le *net* par un annonceur habile, qui attire votre attention et vous incite à cliquer sur des messages insolites ou attrayants, derrière lesquels se dissimulent en réalité des pages publicitaires. Parfois même, certains sites prétendent vous fournir une information objective (par exemple, des conseils diététiques, esthétiques ou médicaux), alors qu'ils sont financés par un annonceur en vue de vous orienter vers ses produits ou services.

En réalité, ces pratiques sont interdites par la loi, qui exige l'identification claire de toute publicité (bannière, message *pop up*, e-mail, information promotionnelle…), et ce, dès sa réception.

Cela signifie que le caractère promotionnel de ce genre de message devrait apparaître de manière évidente, notamment par l'apposition d'une mention "publicité".

Ainsi, dans la présentation du site, aucune confusion ne peut être possible entre information et promotion. En outre, l'annonceur, pour le compte duquel la publicité est faite, doit être clairement identifiable.

124. Qu'en est-il des offres promotionnelles, des concours et des jeux promotionnels sur les réseaux ?

Les offres promotionnelles faites sur Internet doivent toujours être clairement identifiables comme telles. Par offre promotionnelle, on entend les annonces de réduction de prix, ainsi que les offres conjointes, c'est-à-dire des offres qui vous donnent droit, lors de l'achat d'un produit ou d'un service, à un bon de réduction, à un cadeau, à un produit ou à un service gratuit, etc.

Les conditions pour pouvoir bénéficier de ces offres doivent être aisément accessibles (par exemple en cliquant sur un hyperlien) et rédigées en des termes précis et non équivoques. En outre, en cas de réduction de prix, le prestataire a l'obligation d'indiquer l'ancien prix ou le prix habituel, à proximité du prix réduit.

Quant aux concours et autres jeux promotionnels organisés par des annonceurs sur les réseaux, ils doivent également être clairement identifiables. Vous devez en outre pouvoir accéder facilement aux conditions de participation. Celles-ci doivent être présentées de manière précise et non équivoque.

125. Quelles informations dois-je recevoir avant de passer commande ?

Lorsque vous contractez sur Internet, deux difficultés se posent : d'une part, vous n'avez pas de contact direct et concret avec le bien qui est offert, d'autre part, vous devez suivre un processus automatisé de conclusion du contrat. Dès lors, afin d'éviter les erreurs et les malentendus, le prestataire doit vous fournir un certain nombre d'informations avant que vous ne passiez commande chez lui, si vous contractez pour vos besoins propres (et non dans un cadre professionnel).

Il doit d'abord vous informer sur les produits ou services qu'il fournit, ainsi que sur les modalités du contrat, c'est-à-dire les informations suivantes :

- les informations concernant son identité et son activité professionnelle (*supra*, n° 122) ;

- les caractéristiques essentielles du produit ou du service ;
- le prix du produit ou du service, en indiquant si les taxes et les frais de livraison sont inclus ;
- les frais de livraison, le cas échéant ;
- les modalités de paiement (*infra*, n^{os} 156 et s.), de livraison ou d'exécution du contrat ;
- l'existence ou l'absence d'un droit de renonciation (*infra*, n^{os} 144 et s.) ;
- les modalités de reprise ou de restitution du produit, y compris les frais éventuels y afférents ;
- le coût de l'utilisation de la technique de communication à distance, s'il ne correspond pas au tarif de base (c'est-à-dire si la visite du site vous coûte plus que le tarif de connexion de base, p. ex. pour un site dont l'accès est payant) ;
- la durée de validité de l'offre ou du prix ;
- dans le cas de fourniture durable ou périodique d'un produit ou d'un service, la durée minimale du contrat (p. ex., abonnement à un magazine).

Il doit également vous fournir un certain nombre d'informations vous permettant de vous y retrouver sur son site, c'est-à-dire :

- les langues proposées pour la conclusion du contrat ;
- les différentes étapes techniques à suivre pour conclure le contrat (*infra*, n° 129) ;
- la manière de corriger les éventuelles erreurs commises dans la saisie des données, avant que la commande ne soit passée (*infra*, n° 130) ;
- l'archivage éventuel du contrat conclu et, le cas échéant, les conditions d'accès à cette archive après la passation de la commande (*infra*, n° 128).

Ces informations doivent vous être fournies de manière claire, compréhensible et non équivoque.

Sachez que si vous contractez à des fins professionnelles, le prestataire n'est pas obligé de vous fournir toutes ces informations.

126. Les conditions générales doivent-elles m'être communiquées avant la conclusion du contrat ?

Non, mais si elles ne vous ont pas été communiquées avant de conclure le contrat, elles ne peuvent vous être opposées.

En d'autres termes, le prestataire ne peut invoquer contre vous des conditions générales que vous n'avez pas eu la possibilité de consulter et d'accepter avant la conclusion du contrat. Par exemple, il ne pourrait vous opposer des clauses contractuelles qui ne figuraient pas sur son site web et qu'il ne vous a pas communiquées par tout autre moyen avant la conclusion du contrat. Un juge pourrait même estimer que les conditions générales n'ont pas été communiquées si elles ne sont pas suffisamment visibles sur le site web. Ce

pourrait être le cas si elles étaient perdues au fin fond du site, de sorte que seule une recherche minutieuse, ou un heureux hasard, permettait de les trouver.

Toutefois, de nombreux sites offrant des services en ligne affichent leurs conditions générales. Celles-ci sont souvent accessibles par un hyperlien placé sur chacune des pages du site ou à côté du récapitulatif de votre commande. Parfois, au cours du processus de commande, vous devez obligatoirement passer par la page des conditions générales et cliquer sur une icône “J’accepte” pour pouvoir continuer votre commande.

Sachez que, par ce simple clic, vous marquez votre accord sur ces conditions, qui pourront dès lors vous être opposées par le prestataire. Aussi, il vous est vivement recommandé de lire attentivement les conditions générales du prestataire avant de conclure le contrat. Il est plus prudent d’en conserver également une copie, en les imprimant ou en les enregistrant sur votre disque dur ou sur une disquette. D’ailleurs, en vertu de la loi, si le prestataire vous communique ses conditions générales, il doit vous permettre de les conserver et de les reproduire.

127. Quelles informations doivent m’être fournies après la commande ?

Postérieurement à la passation de la commande sur un site web, il est important que vous sachiez si votre commande a bien été enregistrée par le prestataire. C’est pourquoi le prestataire a l’obligation de vous faire parvenir, sans délai injustifié, un accusé de réception, contenant un récapitulatif de votre commande. Celui-ci peut prendre la forme d’une page web s’affichant au terme du processus de commande, ou d’un courrier électronique qui vous serait envoyé dans les plus brefs délais.

En outre, le prestataire doit vous faire parvenir un document confirmant toutes les informations relatives au contrat :

- l’identité et l’adresse géographique du vendeur ;
- le prix du produit ou du service ;
- les frais de livraison, le cas échéant ;
- les modalités de paiement (*infra*, n^{os} 156 et s.), de livraison ou d’exécution du contrat ;
- la durée de validité de l’offre ou du prix ;
- dans le cas de fourniture durable ou périodique d’un produit ou d’un service, la durée minimale du contrat ;
- l’adresse géographique où vous pourrez adresser une plainte ;
- les informations relatives au service après-vente et aux garanties commerciales existants (*infra*, n° 178) ;
- dans le cadre d’un contrat à durée indéterminée ou d’une durée supérieure à 1 an, les conditions dans lesquelles vous pouvez résilier le contrat ;
- l’existence ou l’absence d’un droit de renonciation (*infra*, n° 144) et les modalités et conditions d’exercice de ce droit.

A cet égard, l'une des deux clauses suivantes, rédigée en caractères gras, dans un cadre distinct du reste du texte, doit figurer en première page du document, ou en tout cas de manière bien visible :

- si vous avez un droit de renonciation: "Le consommateur a le droit de notifier au vendeur qu'il renonce à l'achat, sans pénalités et sans indication du motif, dans les … jours ouvrables (au minimum 7 jours) à dater du lendemain du jour de la livraison du produit ou de la conclusion du contrat de service".

- si vous n'avez pas de droit de renonciation: "Le consommateur ne dispose pas du droit de renoncer à l'achat".

Si vous avez acheté un produit, ces informations doivent vous parvenir au plus tard au moment de la livraison.

Si vous avez conclu un contrat portant sur une prestation de service, ces informations doivent normalement vous parvenir avant l'exécution du contrat. Toutefois, si l'exécution du contrat a commencé, avec votre accord, avant la fin du délai de renonciation (de minimum 7 jours), ces informations doivent vous parvenir pendant l'exécution du contrat. Par exemple, s'agissant d'un logiciel téléchargeable en ligne, les informations précitées doivent vous être fournies avant ou, au plus tard, pendant le téléchargement.

Ces informations sont importantes, car elles peuvent vous permettre de vérifier l'exactitude de votre commande, l'étendue de vos droits, les modalités pratiques d'exécution du contrat, mais également toutes les démarches à suivre en cas de problème : renonciation au contrat, réclamation, service après-vente, garanties, etc.

Il est donc important de garder le document contenant ces informations, qui pourrait également constituer un précieux moyen de preuve en cas de contestation (*infra*, n° 133). Afin de vous permettre de conserver ces informations et de les consulter ultérieurement, le prestataire doit vous les faire parvenir sur un support durable. Il peut s'agir d'un simple document papier, voire d'un CD-ROM ou d'une disquette, envoyé par la poste ou joint à votre colis, ou encore d'un courrier électronique ou d'un fax.

Notez que si vous contractez à des fins professionnelles, le prestataire n'est pas obligé de vous fournir ces informations.

128. Puis-je suivre l'évolution de ma commande après la conclusion du contrat ?

Si le prestataire vous offre la possibilité d'accéder à une copie archivée de votre commande, il doit vous en informer clairement avant la passation de la commande.

Ainsi, certains prestataires vous permettent de consulter, sur leur site, l'état d'avancement de votre commande, les précédentes commandes que vous avez passées chez eux, les différentes données personnelles vous concernant qui ont été enregistrées, etc. Parfois, il est même possible de modifier, voire d'annuler une commande déjà enregistrée, tant qu'elle n'a pas encore été exécutée. Lorsque c'est le cas, le prestataire vous en informe sur son site ou dans l'accusé de réception de la commande.

CHAPITRE II. LA CONCLUSION D'UN CONTRAT SUR INTERNET

129. Comment passer commande sur un site web ?

Afin de vous permettre d'évoluer en toute confiance sur son site, le prestataire a l'obligation de vous informer de la marche à suivre pour passer commande, étape par étape (*supra*, n° 125). Notez que si vous contractez à des fins professionnelles, le prestataire peut déroger à cette obligation.

Généralement, la procédure de commande se déroule comme suit (la procédure décrite ci-dessous n'est qu'un exemple, parmi d'autres, de processus de commande en ligne).

Pour commencer, vous pouvez trouver le produit ou le service que vous désirez en consultant, le cas échéant, un catalogue en ligne, disponible sur le site du prestataire et reprenant par rubriques l'ensemble des produits et services offerts en vente. La consultation de ce catalogue est parfois facilitée par l'utilisation d'un moteur de recherche. Au fur et à mesure de vos recherches, vous pouvez sélectionner un ou plusieurs articles, qui s'accumulent dans votre "panier d'achats".

Une fois votre choix arrêté, vous pouvez décider d'amorcer le processus de conclusion du contrat, en cliquant sur une icône spécifique. Vous êtes alors invité à suivre un itinéraire qui, dans le meilleur des cas, est soigneusement découpé en étapes, chaque passage à l'étape ultérieure étant conditionné par votre approbation, exprimée par un clic sur l'icône appropriée. A chaque instant, si vous le désirez, vous avez la possibilité d'interrompre la procédure et de revenir en arrière, sans conclure le contrat.

Ainsi, pas à pas, vous allez remplir le formulaire de commande, introduire vos données à caractère personnel, choisir votre mode de paiement et de livraison, etc. En cours de route, vous pouvez accéder à une foule d'informations, concernant les conditions générales de vente, les tarifs et délais de livraison, les taxes éventuelles, la protection de vos données à caractère personnel, etc.

Une fois déterminés tous les éléments du contrat, de nombreux sites prévoient qu'un récapitulatif de l'opération apparaît à l'écran. Il est vivement recommandé de vérifier une dernière fois l'exactitude des données, avant de valider définitivement la commande, en cliquant sur l'icône prévue à cet effet. Ce n'est qu'au terme de ce processus que la commande est enregistrée. Parfois, une page web s'affiche à l'écran pour vous confirmer l'enregistrement de votre commande (*supra*, n° 127).

De nombreux prestataires fournissent sur leur site des informations destinées à vous familiariser avec l'achat en ligne. La page d'accueil présente parfois une "visite guidée" du site proposant une simulation de commande. Souvent, on peut également trouver une foule d'informations sur le fonctionnement du site, les modalités d'achat, les solutions en cas de problèmes, les astuces de navigation, etc., dans une rubrique d'aide, accessible depuis la page d'accueil, ou en bas de chaque page.

130. Comment m'assurer que je n'ai pas commis d'erreur dans ma commande ?

Il peut arriver à tout le monde de se tromper : sélectionner le mauvais article, ou le sélectionner plusieurs fois, commettre une erreur au moment de compléter le formulaire de commande dans le numéro de carte de crédit, l'adresse de livraison, etc.

Afin d'éviter que la commande que vous envoyez contienne des inexactitudes, la loi oblige le prestataire à mettre en œuvre sur son site des moyens permettant d'identifier et de

corriger les éventuelles erreurs que vous auriez commises dans la saisie des données. Attention : si vous contractez à des fins professionnelles, le prestataire peut déroger à cette obligation.

Certains sites utilisent des logiciels programmés de manière à détecter automatiquement les erreurs manifestes dans l'enregistrement de la commande : quantités exorbitantes, données incompatibles avec la définition d'un champ, introduction de données contradictoires, numéro de carte de crédit incorrect, absence d'indication du nom ou de l'adresse de livraison… Un message d'erreur apparaît alors, vous invitant à opérer les corrections nécessaires.

En outre, le prestataire peut facilement réduire les risques en plaçant, tout au long du processus de commande, depuis la sélection d'un article jusqu'à la validation de la commande, des boutons de correction, de modification, d'annulation, de suppression des divers éléments de la commande. Ainsi, vous pouvez modifier votre commande à tout moment, si vous détectez une erreur ou simplement si vous changez d'avis.

Souvent, on l'a vu (*supra*, n° 129), l'achat se clôture par l'affichage d'une page de confirmation, pour vous permettre de vérifier l'exactitude des données enregistrées avant de valider le tout.

Si, malgré toutes ces précautions, vous vous rendez compte, à l'exécution du contrat, que vous avez commis une erreur dans votre commande, vous disposez encore, dans de nombreux cas, d'un droit de renonciation (*infra*, n^{os} 144 et s.).

131. A partir de quand suis-je engagé contractuellement ?

La solution à cette question diffère en fonction du droit applicable au contrat (*infra*, n^{os} 194 et s.), selon que l'on considère votre commande comme une acceptation de l'offre du prestataire ou comme une offre faite au prestataire. Nous n'examinons ici que quelques possibilités.

Si le droit belge est applicable, votre commande signifie que vous acceptez l'offre que le prestataire (établi en Belgique) vous a faite sur son site de commerce électronique (ou par e-mail). Le contrat est donc conclu au moment où votre commande parvient au prestataire. En droit français, la conclusion du contrat a lieu au moment où vous validez votre commande. En pratique, cela revient à peu près au même, étant donné qu'il ne s'écoule que quelques secondes entre ces deux instants.

Par contre, selon les droits allemand et anglais, votre commande représente une offre de contracter, que vous envoyez au prestataire et qu'il a encore le loisir de refuser ou d'accepter. Le contrat n'est donc conclu qu'au moment où vous recevez un message du prestataire acceptant votre offre. Le plus souvent, il manifestera son acceptation en exécutant le contrat. Notez qu'en principe, vous êtes engagé par votre offre et ne pouvez plus la retirer. Néanmoins, il vous reste la possibilité d'exercer votre éventuel droit de renonciation si vous changez d'avis par la suite (*infra*, n^{os} 144 et s.).

Face à ces différences de régimes, vous devrez donc être attentif au droit applicable au contrat.

132. Comment être certain que le prestataire a bien reçu ma commande ?

Lorsque vous passez commande sur un site web, il est important que vous sachiez si votre commande a bien été enregistrée par le prestataire. Rappelons que le prestataire a

l'obligation de vous faire parvenir, sans délai injustifié, un accusé de réception, contenant un récapitulatif de votre commande (*supra*, n° 127). Il peut prendre la forme d'une page web s'affichant au terme du processus de commande ou d'un courrier électronique qui vous serait envoyé dans les plus brefs délais.

Attention : si vous contractez à des fins professionnelles, le prestataire peut déroger à cette obligation.

CHAPITRE III. LA PREUVE ET LA SIGNATURE ELECTRONIQUE

Vous avez conclu un contrat par Internet et avez veillé à ce que le processus prévu pour la formation du contrat soit respecté. Vous vous demandez toutefois si, par cette commande, vous êtes engagé de la même façon que par un écrit traditionnel et plus particulièrement s'il vous sera aisé d'en faire la preuve.

Oui, sur le plan des principes. Deux lois récentes (lois du 20 octobre 2000 et du 9 juillet 2001) visent à assurer la reconnaissance juridique des mécanismes de signature électronique. Sachez toutefois que cette reconnaissance juridique ne s'applique pas à toutes les techniques de signature électronique et que des conditions strictes doivent être respectées. Nous nous proposons d'apporter de manière pragmatique des éclaircissements sur ce sujet.

Que se passe-t-il si un litige survient entre vous (consommateur) et le vendeur à propos de l'existence ou du contenu du contrat ? Une distinction est à opérer selon que la contestation est soulevée par vous-même ou par le vendeur.

133. Comment puis-je faire la preuve que j'ai passé commande par Internet ?

Si, en tant que consommateur, vous voulez apporter la preuve que vous avez passé commande à l'égard d'un vendeur-commerçant (la règle est différente s'il s'agit d'un vendeur particulier), vous bénéficiez du régime de la liberté de preuve. En d'autres termes, vous pouvez utiliser tout moyen pour tenter de démontrer que vous avez effectivement passé commande. Comment ? En fournissant notamment une copie électronique de votre bon de commande et de la confirmation (par courrier électronique par exemple) de la commande qui vous a été transmise par le vendeur. Sachez toutefois qu'il appartient au juge d'apprécier la valeur du document que vous lui présenterez en cas de litige. Soyez donc vigilant ! Pour les commandes importantes, privilégiez un système sécurisé de signature électronique.

Deux conseils donc :

- Conservez toujours une copie (papier ou électronique suivant le cas) de votre bon de commande ainsi que de la confirmation du vendeur !

- Pour les commandes importantes, utilisez un système de signature électronique répondant à l'ensemble des conditions de la loi afin de bénéficier de l'assimilation à la signature manuscrite (comme expliqué ci-après).

134. Comment le vendeur peut-il prouver que j'ai passé commande par Internet ?

Disons-le d'emblée, la preuve de l'existence du contrat sera plus ardue pour le vendeur (sauf si vous avez payé le vendeur ! Dans ce cas, il sera plus facile pour celui-ci d'en faire la preuve).

Une distinction est à opérer selon que le montant total de votre commande est inférieur (ou égal) ou supérieur à 375,00 EUR.

Dans le premier cas, le vendeur bénéficie du régime de la liberté de preuve. Il pourra donc se prévaloir du bon de commande que vous avez rempli, même si ce dernier se présente sous une forme électronique et n'est pas signé. Mais il est vrai que le juge pourrait ne pas lui reconnaître une valeur probatoire en raison du manque de sécurité qui entoure la génération de celui-ci.

Dans le second cas, le vendeur devrait normalement être en possession d'un écrit signé. A l'heure actuelle, on entend par écrit signé non seulement un écrit papier signé à la main, mais aussi un écrit signé à l'aide d'un mécanisme de signature électronique pour autant que cette signature électronique réponde aux conditions consacrées par la loi. S'il ne se procure pas l'une ou l'autre de ces techniques de signature, on peut dès lors craindre que la preuve de la commande et de la conclusion du contrat (ainsi que de son contenu) sera pour lui difficile à apporter.

Rappelons également que le vendeur en ligne est tenu d'accuser réception de la commande du destinataire sans délai injustifié et par voie électronique, et ce, quel que soit le montant de la commande. Par ailleurs, il lui appartient en cas de contestation d'apporter la preuve qu'il a effectivement accusé réception de cette commande.

135. Un simple courrier électronique est-il reconnu comme une preuve ?

On peut raisonnablement estimer que le courrier électronique simple constitue tout au plus une présomption et/ou un commencement de preuve par écrit. La particularité de ces deux moyens de preuve est qu'ils doivent nécessairement être complétés par d'autres moyens de preuve pour pouvoir convaincre le juge. On dit dans le jargon juridique qu'ils sont des moyens de preuve "imparfaits". Dès lors, si vous ne pouvez vous prévaloir que d'un courrier électronique simple (non complété par d'autres indices ou des témoignages), il est fort probable que ce dernier, à lui seul, ne permette pas de convaincre le juge quant à la réalité ou au contenu du contrat, à tout le moins s'il est contesté. Cela s'explique par la relative insécurité entourant la création et l'envoi d'un courrier électronique simple et par les nombreuses possibilités de falsification.

Si le courrier électronique n'est pas accompagné d'une signature électronique, on considérera généralement qu'il ne s'agit pas d'un écrit signé au sens de la loi, à moins que la jurisprudence adopte une position différente prochainement. Dès lors, lorsque la loi exige un écrit signé pour faire preuve (notamment à l'égard d'un particulier d'un acte juridique qui excède 375,00 EUR), on peut raisonnablement affirmer que le courrier électronique simple ne répond pas à cette condition.

Un bémol doit néanmoins être apporté à cette affirmation. En effet, les dispositions relatives à la preuve ne sont pas d'ordre public. Il est dès lors possible, préalablement à toute relation contractuelle par voie électronique, de traiter dans un contrat les questions relatives à l'admissibilité et à la valeur probante des documents électroniques. L'on pourrait imaginer dans ce cadre que les parties prévoient par exemple un régime d'équivalence entre un courrier électronique ou un téléfax et un écrit papier signé à la main. Une telle convention est généralement valable et a pour effet d'interdire aux parties de contester trop facilement, après coup, la valeur probatoire de ces documents électroniques.

Ce type de clause est fréquent (relations banques-clients par exemple). Par conséquent, si vous souhaitez contester la valeur juridique d'un courrier électronique ou d'un téléfax envoyé par votre vendeur, vérifiez auparavant que vous n'avez pas signé lors du démarrage de la relation d'affaires avec le vendeur une convention contenant ce type de clause !

136. Un document signé électroniquement est-il un moyen de preuve efficace ?

L'un des intérêts pour un internaute de recourir à une signature électronique est d'avoir la certitude que le document signé pourra faire preuve au même titre qu'un document papier revêtu d'une signature classique (manuscrite). Dans ce contexte, il convient de préciser

quelles sont les conditions à remplir pour qu'une signature électronique soit assimilée d'office à une signature manuscrite.

Pour pouvoir compter sur l'assimilation automatique, profiter des effets juridiques déjà reconnus à la signature manuscrite et bénéficier ainsi d'une sécurité juridique satisfaisante, une signature électronique doit répondre aux conditions cumulatives suivantes :

- la signature électronique doit être *avancée* au sens de la loi du 9 juillet 2001 sur la signature électronique ;
- la signature électronique avancée doit être basée sur un *certificat qualifié* : il s'agit d'un certificat ayant un contenu minimal prévu par la loi (annexe I de la loi du 9 juillet 2001) et émis par un prestataire de service de certification respectant un ensemble de conditions strictes consacrées par la loi (annexe II de la même loi) ;
- la signature électronique doit être conçue au moyen d'un dispositif *sécurisé* de création de signature électronique : un dispositif de création de signature n'est considéré comme *sécurisé* que s'il satisfait aux exigences de l'annexe III de la loi du 9 juillet 2001.

Afin de vous permettre de comprendre l'intérêt de ces conditions et le rôle de chaque acteur, voyons méthodiquement ce qu'est une signature électronique avancée et comment fonctionne une signature numérique, quel est le rôle d'un prestataire de service de certification, ce qu'est un certificat numérique (qualifié), ce qu'est un dispositif sécurisé de création de signature électronique et comment tout cela fonctionne concrètement.

137. Qu'est-ce qu'une signature électronique avancée ?

La loi définit la " *signature électronique avancée* " comme "*une donnée électronique, jointe ou liée logiquement à d'autres données électroniques, servant de méthode d'authentification et satisfaisant aux exigences suivantes :*

a) être liée uniquement au signataire;

b) permettre l'identification du signataire;

c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif;

d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée".

Cette définition est libellée en des termes généraux afin d'assurer une neutralité technique et de ne pas privilégier une technologie ou l'autre existant sur le marché. En pratique, il n'est cependant pas toujours aisé de déterminer si les différents mécanismes techniques de signature électronique tels que la signature biométrique, le code secret associé à l'utilisation d'une carte et la signature numérique (ou digitale) répondent à l'ensemble des conditions de la définition. Ceci dit, tous les commentateurs s'accordent à dire que la signature numérique fondée sur la cryptographie asymétrique et utilisée dans le cadre d'une infrastructure à clé publique (comme celle offerte par Isabel, Globalsign ou Belgacom E-Trust par exemple) répond à cette notion de signature électronique avancée. Dans la mesure où cette technologie s'impose actuellement sur le marché et est privilégiée dans le cadre des projets *e-Government* (notamment le projet relatif à la carte d'identité électronique)

mis en place par notre gouvernement, il paraît important de montrer comment fonctionne ce système de signature.

La signature dite numérique ou digitale repose sur les procédés de cryptographie asymétrique ou “à clé publique”. Dans un système à clé publique, la réalisation de la fonction d’identification suppose qu’une personne dispose de deux clés mathématiques complémentaires : une clé privée dont le caractère secret doit effectivement être préservé et une clé publique qui peut être librement distribuée. Ces deux clés sont générées sur la base d’une fonction mathématique telle qu’il est impossible dans un laps de temps et avec des moyens raisonnables de découvrir la clé privée au départ de la clé publique correspondante. La clé publique doit dès lors représenter une fonction irréversible de la clé privée. La clé privée permet de “signer” le message. L’opération de décodage s’effectue, quant à elle, selon le principe de la complémentarité des clés : un message encodé avec une clé privée ne peut être décodé qu’à l’aide de la clé publique complémentaire. L’identité du signataire est confirmée par un certificat, émis par un prestataire de service de certification (PSC), qui atteste l’identité du signataire et le fait que la clé publique en question lui appartient effectivement.

L’exemple suivant illustre le fonctionnement de la signature numérique.

Alice désire envoyer à Bernard un message informatisé signé à l’aide d’une signature numérique[2]. Après avoir écrit son message, Alice réalise un condensé du message au moyen d’une opération mathématique. Ce condensé est le résultat d’une fonction appelée fonction de hachage irréversible. Cette fonction permet de générer de façon concise une chaîne de données qui représente le message en question. Cette représentation permet de détecter tout changement apporté au message. En effet, il suffit au destinataire d’appliquer la fonction de hachage au message reçu et de comparer le condensé ainsi obtenu avec celui transmis par l’émetteur. Toute différence entre les condensés signifie que le message a été altéré en cours de transmission.

Ce condensé est par la suite encodé (rendu illisible et inaccessible) à l’aide de la clé privée d’Alice. Ce condensé encodé constitue la signature numérique (ou digitale). Alice envoie alors à Bernard son message (en clair) accompagné de la signature numérique.

---

[2] Pour assurer la confidentialité d’un échange, l’expéditeur procédera inversement : il chiffrera le message à l’aide de la clé publique du destinataire, qui pourra uniquement le déchiffrer au moyen de sa propre clé secrète. Ainsi sera-t-il le seul à pouvoir prendre connaissance du message. Il va de soi que les deux fonctions peuvent être combinées pour l’envoi d’un message à la fois confidentiel et signé.

Lorsque Bernard reçoit le message et la signature numérique, il décode cette dernière en effectuant une opération mathématique impliquant la clé publique complémentaire d'Alice. S'il parvient à décoder la signature, Bernard est assuré que celle-ci a préalablement été réalisée avec la clé privée complémentaire d'Alice : il sait alors de manière certaine qu'elle est l'auteur du message pour autant qu'une partie tierce (une autorité de certification ou prestataire de service de certification) certifie que cette clé publique est bien celle d'Alice (*infra*, n° 142). Grâce à la fonction de hachage[3] et à la comparaison des deux "empreintes", l'intégrité du message d'Alice peut être vérifiée.

Il convient de souligner, qu'en réalité, toutes ces opérations sont effectuées en un bref laps de temps par votre logiciel de signature électronique.

Reste à préciser que l'utilisation de la cryptographie à clé publique suppose l'organisation de la publicité des clés publiques et l'instauration d'un mécanisme de contrôle visant à s'assurer en permanence que celles-ci correspondent bien aux personnes qui s'en prétendent titulaires. Cette double mission de publicité et de certification est actuellement assumée par un tiers certificateur (appelé "prestataire de service de certification" ou encore "autorité de certification").

138. Qu'est-ce qu'un prestataire de service de certification ?

Le prestataire de service de certification (ci-après PSC) est un organisme indépendant habilité, d'une part, à *vérifier l'identité* des titulaires de clé publique[4] et à *générer des certificats*, sortes d'attestations électroniques qui font le lien entre une personne et sa clé publique, et, d'autre part, à *assurer la publicité* la plus large des certificats ainsi émis. Le PSC est également tenu de maintenir à jour le répertoire contenant les certificats de clé publique, en veillant, le cas échéant, à leur révocation. Ce tiers à la communication électronique joue un rôle capital pour assurer la fiabilité de la signature numérique et l'identification des intervenants, en vue d'échanges contraignants dans les réseaux ouverts.

On l'a vu, la principale fonction d'un PSC est d'assurer un lien formel entre une personne et sa clé publique, moyennant l'émission d'un certificat. Ce certificat contient ainsi différentes informations relatives notamment à l'identité du titulaire du certificat (celui qui veut signer et s'identifier comme tel) et à sa clé publique. Le certificat est signé par le PSC à l'aide de sa propre clé privée et est, de ce fait, protégé contre les altérations.

L'exemple suivant illustre l'utilisation possible de certificats. Alice transmet à Bernard un message ainsi que sa signature numérique réalisée à l'aide de sa clé privée. Après avoir reçu ces documents (soient deux fichiers informatiques liés : le message et la signature

---

3 Remarquons toutefois que la réalisation d'un condensé du message à l'aide de la fonction de hachage irréversible n'est pas indispensable. En effet l'émetteur du message pourrait directement encoder le message avec sa clé privée sans nécessairement passer par la production du condensé. Néanmoins la fonction de hachage irréversible sera souvent utilisée pour des raisons informatiques dans un souci de gagner du temps : encoder avec la clé privée un condensé (fichier de petite taille) est plus rapide que l'encodage du message en clair (fichier de plus grosse taille).

4 Notons que l'ensemble des certificats délivrés par un PSC ne sont pas nécessairement des certificats d'identité. Certains certificats peuvent être anonymes ou ne concerner que des attributs. Toutefois, dans la matière qui nous occupe, à savoir celle de l'utilisation des certificats à des fins de signature, nous ne traiterons que des certificats d'identité.

numérique), Bernard commence par vérifier le certificat (qu'il aura reçu d'Alice ou qu'il aura été chercher dans un répertoire électronique de certificats) à l'aide de la clé publique du PSC. Si la vérification s'avère concluante, il est assuré de l'intégrité des informations contenues dans le certificat (l'identité d'Alice et sa clé publique). Il peut ensuite utiliser la clé publique d'Alice pour vérifier la signature du message transmis par celle-ci. Bernard sera alors certain que le message émane réellement d'Alice.

Le PSC peut remplir d'autres fonctions qui sont subsidiaires à la certification : l'archivage des informations qui sont relatives aux certificats (surtout pour des questions de preuve) ; le cas échéant, la génération de la paire de clés, sans toutefois conserver copie de la clé privée ; la tenue d'un registre électronique de certificats accessible au public ; l'horodatage de messages signés numériquement ; l'archivage de documents électroniques, etc.

En Belgique, il existe actuellement plusieurs prestataires de service de certification, dont notamment Globalsign (http://www.globalsign.net), Belgacom E-Trust (http://www.e-trust.be) et Isabel (http://www.isabel.be).

139. Qu'est-ce qu'un certificat numérique qualifié ?

Comme indiqué précédemment, un certificat n'est rien d'autre qu'une attestation électronique qui lie une personne physique ou morale à sa clé publique et confirme l'identité de cette personne. Par l'émission du certificat, le prestataire de service de certification "certifie" ce lien et affirme publiquement l'exactitude des informations qu'il contient.

Nous indiquions également que pour pouvoir bénéficier de l'assimilation automatique de la signature électronique à la signature manuscrite, l'utilisateur doit notamment recourir à un certificat *qualifié*. Le certificat est élevé au rang de *certificat qualifié* s'il satisfait aux exigences visées à l'annexe I – c'est-à-dire s'il contient un minimum d'informations – et s'il est fourni par un PSC satisfaisant aux exigences visées à l'annexe II – c'est-à-dire s'il a été émis dans de bonnes conditions de sécurité (l'annexe II contient des garanties de sécurité, de fiabilité, d'information, financières et probatoires).

Si un opérateur estime qu'il respecte ces conditions (dont certaines sont libellées en termes très généraux), il peut délivrer des certificats qualifiés. Toutefois, le respect effectif de ces conditions ne fait l'objet d'aucun contrôle *a priori* par l'Administration ou une autre autorité indépendante. Tout au plus, la loi oblige-t-elle ces opérateurs à faire une déclaration préalable à l'Administration. Cette obligation de déclaration vise notamment à permettre à l'Administration d'exercer son pouvoir de contrôle *a posteriori* consacré par la loi.

A ce jour en Belgique, seuls Belgacom E-Trust et GlobalSign délivrent des certificats "*qualifiés*" (cette information est disponible sur le site du Service public fédéral Economie, PME, Classes moyennes et Energie : http://mineco.fgov.be/information_society/index_fr.htm).

140. Qu'est-ce qu'un dispositif sécurisé de création de signature électronique ?

Nous avons vu que la dernière condition pour qu'une signature électronique puisse bénéficier de l'assimilation automatique à la signature manuscrite est l'utilisation d'un dispositif *sécurisé* de création de signature.

La notion de dispositif de création de signature est définie par la loi comme un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature (c'est-à-dire la clé privée). Plus concrètement, cela vise par exemple le logiciel qui permet de générer les données afférentes à la création et à la vérification de

signature (clé privée/clé publique), celui qui permet de créer et/ou de vérifier une signature électronique, la carte à puce sur laquelle sont stockées les données afférentes à la création de signature, le lecteur de carte à puce, etc.

Les dispositifs de création de signature ne sont considérés comme *sécurisés* que s'ils satisfont aux exigences de l'annexe III de la loi. Ces dernières sont libellées en termes très généraux : les dispositifs doivent garantir l'unicité et le maintien de la confidentialité des données utilisées pour créer la signature électronique ; les dispositifs doivent rendre impossible la déduction des données utilisées pour créer la signature à partir de celles utilisées pour vérifier la signature (connues de tous) ; les dispositifs doivent rendre impossible la falsification de la signature ; les dispositifs doivent donner la possibilité au "signataire" de protéger techniquement (par un mot de passe ou un contrôle biométrique par exemple) les données utilisées pour créer la signature afin d'empêcher tout accès illégitime à celles-ci. Enfin, ces dispositifs ne doivent pas modifier les données à signer ni empêcher que ces données soient soumises au "signataire" avant le processus de signature. Il apparaît en effet indispensable que le signataire puisse visualiser, vérifier le contenu, repérer d'éventuelles modifications, et ainsi adhérer à ce qu'il signe.

Pour le fabriquant de tels dispositifs, il n'est toutefois pas aisé *en pratique* de déterminer à quelles exigences techniques ils doivent correspondre pour pouvoir revendiquer le statut de dispositif *sécurisé*. Néanmoins, selon la loi, la Commission européenne attribuera et publiera au *J.O.C.E.* des numéros de référence de normes généralement admises pour des produits de signature électronique. Lorsqu'un produit de signature électronique est conforme à ces normes, il est *présumé satisfaire* aux exigences de l'annexe III. Par ailleurs, la loi ajoute que "la conformité des dispositifs sécurisés de création de signature électronique par rapport aux exigences visées à l'annexe III de la présente loi est attestée par des organismes compétents désignés par l'Administration et dont la liste est communiquée à la Commission européenne". Le paragraphe 3 indique que les conditions auxquelles doivent répondre ces organismes seront déterminées par un arrêté royal. De plus, la conformité établie par un organisme désigné par un autre État membre de l'Espace économique européen est également reconnue en Belgique.

Suivant une interprétation communément admise de l'article 3, § 4, de la Directive "signature électronique", cette conformité aux exigences de l'annexe III ne doit pas être démontrée *a priori*, c'est à dire avant la mise sur le marché des dispositifs. Les fabricants peuvent donc mettre sur le marché des dispositifs de création de signature qu'ils déclarent "sécurisés". Cela signifie qu'en cas de litige relatif au contrat signé par de tels dispositifs, une contestation peut naître quant au caractère sécurisé ou non du dispositif utilisé pour signer et donc quant à la valeur probante de la signature. Si tel est le cas, il appartiendra au juge d'établir cette conformité.

141. Comment obtenir un certificat numérique ?

Quelles sont les opérations à effectuer en pratique pour pouvoir obtenir un certificat numérique et signer vos documents électroniques au moyen d'une signature numérique ?

Avant de passer à la démarche de signature, il est généralement nécessaire de se présenter en personne auprès d'un PSC (ou d'une autorité d'enregistrement, sous-traitant du PSC) afin d'obtenir un certificat (moyennant rémunération en général).

Préalablement à l'émission du certificat, le PSC :

- génère une paire de clés (privée et publique) à l'aide d'un logiciel conçu à cet effet et stocke la clé privée par exemple sur une carte à puce protégée par mot de passe, à l'attention du demandeur (il s'agit du procédé de stockage le plus sécurisé) ;
- vérifie l'identité du demandeur à l'aide de documents probants (carte d'identité, passeport, etc.) ainsi que d'éventuelles autres informations destinées à se trouver sur le certificat (profession, qualité d'administrateur délégué d'une société, etc.) ;
- génère le certificat, qui contient au moins l'identité de son titulaire ainsi que sa clé publique ;
- signe le certificat à l'aide de sa clé privée afin, d'une part, de s'identifier comme tel, d'autre part, d'assurer l'intégrité du contenu du certificat ;
- stocke le certificat dans un registre électronique accessible en ligne et en permanence à toute personne intéressée ;
- fournit un exemplaire du certificat numérique au demandeur.

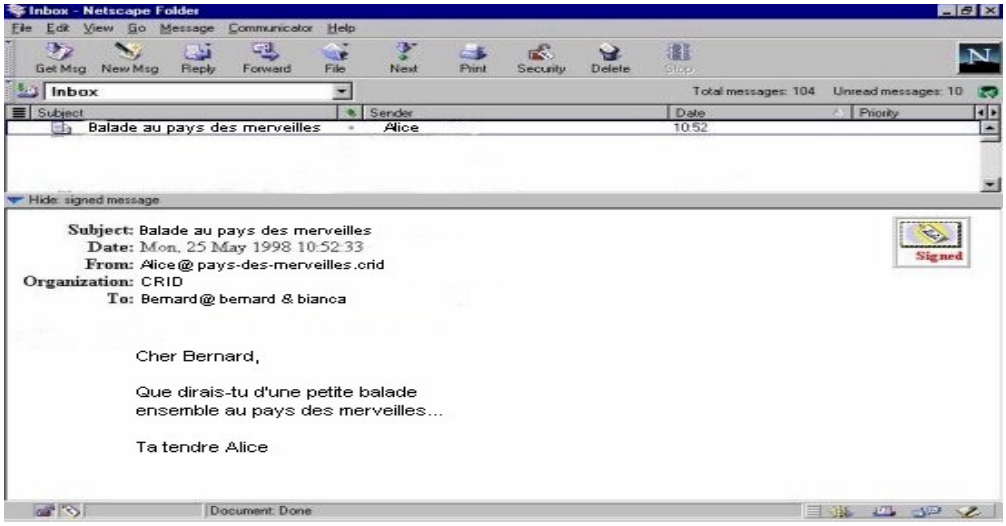
Ensuite, il reste à installer un logiciel disposant d'un module générant des signatures numériques, ce qui est le cas pour les *browsers* récents. Windows 2000 a également intégré un module permettant de générer des signatures numériques. Certaines sociétés ont développé leur propre logiciel (par exemple Isabel). *Notons néanmoins que tous les logiciels n'offrent pas un niveau de protection et de sécurité comparable. Il est donc vivement recommandé de s'adjoindre les conseils d'un expert en la matière.*

142. Comment fonctionne en pratique une signature numérique ?

Une fois votre certificat numérique obtenu, il ne vous reste plus qu'à signer le document rédigé ou à vérifier la signature du document reçu. En pratique, le logiciel effectue automatiquement toutes les opérations présentées de manière théorique précédemment. Le caractère complexe du mécanisme est caché par l'interface logicielle.

Pour reprendre l'exemple évoqué ci-dessus, Alice envoie le message à Bernard. Il lui suffit de rédiger le message, de cocher l'option "signer" et d'envoyer le message ("*send*").

Lorsque Bernard reçoit le message, il lui suffit de vérifier que “l’icône de signature” se trouve dans le coin supérieur droit de l’écran, ce qui atteste que le document a été signé et que la procédure de vérification de signature s’est déroulée correctement.



Pour pouvoir procéder à la procédure de vérification de la signature, le logiciel doit disposer du certificat d’Alice. Soit il faudra le télécharger dans le registre électronique du PSC, soit le certificat était déjà stocké dans le logiciel auquel cas, il convient de vérifier qu’il n’a pas expiré ou n’a pas été révoqué.

Remarquons que l’exemple montré ici n’est pas exclusif. De nombreux autres logiciels offrent des fonctionnalités similaires, mais avec une interface relativement différente.

143. Le recommandé électronique est-il reconnu en droit belge ?

Lorsqu’on envisage la passation d’une transaction électronique, il convient de ne pas se limiter aux problèmes de l’identification des parties et au maintien de l’intégrité du contenu du message. Il faut envisager l’opération juridique dans un tout électronique. Il est dès lors tout aussi important de veiller à conserver la preuve de la réalité d’un envoi ainsi que de la date et, éventuellement, de la réception de celui-ci.

Or cela n’est possible que si, au-delà de la reconnaissance de la signature électronique, le législateur admet le recommandé électronique au même titre que le recommandé “par La Poste”, sous forme papier. En effet, de nombreuses législations ou réglementations imposent l’usage d’une lettre recommandée, avec le cas échéant un accusé de réception, pour l’accomplissement de certaines formalités (notamment dans le cadre d'une procédure judiciaire ou administrative).

Même lorsque cet usage n’est pas requis par la loi, il est souvent utile pour des actes importants de faire usage du recommandé afin de se ménager la preuve de la réalité et de la date d’un envoi ou d’une notification quelconque.

En Belgique, l’usage du recommandé *électronique* est juridiquement possible. Par ailleurs, il est désormais autorisé de recourir à d’autres opérateurs que La Poste pour envoyer des recommandés électroniques.

CHAPITRE IV. LE DROIT DE RENONCIATION

144. Qu'est-ce que le droit de renonciation ?

Lorsque vous achetez à distance, il se peut que vous regrettiez par la suite votre achat, pour différentes raisons : vous avez agi sur un coup de tête ou, à la réflexion, les conditions d'achat ne vous semblent pas très avantageuses, ou tout simplement, le produit livré ne rencontre pas vos attentes…

Sachez que, sauf cas particuliers, en principe, la loi vous donne le droit de renoncer au contrat, dans un délai d'au moins 7 jours ouvrables. Ce droit peut s'exercer de manière discrétionnaire : vous ne devez pas indiquer le motif pour lequel vous avez décidé de renoncer au contrat.

145. Pour quels achats ai-je un droit de renonciation ?

Sous réserve des situations exposées ci-après, vous disposez d'un droit de renonciation pour tout contrat conclu à distance, portant sur la fourniture d'un produit ou d'un service, à condition que vous contractiez à des fins non professionnelles.

Néanmoins, il existe des cas où vous ne disposez pas d'un droit de renonciation :

- si vous demandez l'exécution du service avant l'expiration du délai de renonciation (p. ex., si vous voulez accéder à une base de données et consulter immédiatement les informations demandées, sans attendre la fin du délai de renonciation) ;
- si vous commandez des produits confectionnés selon vos spécifications ou nettement personnalisés pour vous (p. ex., un vêtement confectionné sur commande, un produit marqué de votre nom, des meubles de cuisine agencés selon les mesures de votre cuisine…) ;
- si les produits achetés ne peuvent être réexpédiés ou sont susceptibles de se détériorer ou de se périmer rapidement (p. ex., des denrées périssables, des produits frais, etc.) ;
- si vous achetez des journaux, périodiques ou magazines ;
- si vous faites des paris ou achetez des billets de loterie en ligne ;
- si vous descellez un enregistrement audio ou vidéo ou des logiciels informatiques (p. ex., DVD, CD, CD-ROM, cassette vidéo…). En revanche, si vous ne touchez pas au système de sécurité, vous pouvez renoncer au contrat et restituer le produit intact. Cette exception vaut également pour les enregistrements et les logiciels téléchargeables en ligne, qui sont protégés par des clés d'accès ou un système de sécurité.

Enfin, si votre contrat porte sur l'achat de services financiers (banque, assurance, investissements financiers et boursiers, fonds de pension), vous ne disposez pas, à ce jour, d'un droit de renonciation. Toutefois, une directive européenne sur la commercialisation à distance des services financiers auprès des consommateurs vient d'être publiée et devra prochainement être transposée en droit belge. Cette directive prévoit notamment un droit de renonciation pour certains services financiers, selon des modalités particulières.

146. Comment savoir si je bénéficie ou non d'un droit de renonciation ?

Le prestataire a l'obligation de vous informer de l'existence ou de l'absence d'un droit de renonciation. Cette information doit être préalable à la conclusion du contrat (elle doit, p. ex., figurer sur le site du prestataire) (*supra*, n° 125).

En outre, cette information doit vous être rappelée postérieurement à la conclusion du contrat, lors de la confirmation de certaines informations (p. ex., dans un courrier électronique ou sur la facture accompagnant le produit à la livraison) (*supra*, n° 127).

147. Que puis-je faire si je n'ai reçu aucune information relative à mon droit de renonciation ?

La loi prévoit des sanctions lorsque le prestataire n'a pas rempli son obligation d'information relative au droit de renonciation.

Si, avant la conclusion du contrat, le prestataire ne vous a pas informé de l'*absence* de droit de renonciation (*supra*, n° 125), le délai pour renoncer est alors de 3 mois au lieu de 7 jours (*infra*, n° 148).

Si, postérieurement à la conclusion du contrat, la *clause de renonciation* ne figure pas dans le document vous confirmant un certain nombre d'informations (*supra*, n° 127), la loi assimile le contrat à une vente forcée. En d'autres mots, tout se passe comme si le produit ou le service vous avait été fourni sans demande préalable de votre part : vous n'êtes pas tenu de payer le produit, ni de le restituer.

148. Dans quels délais puis-je renoncer au contrat ?

En principe, vous disposez d'un délai de renonciation de **7 jours** ouvrables minimum. Cela signifie que vous devez notifier au prestataire, avant l'expiration de ce délai, votre intention de renoncer au contrat (*infra*, n° 152).

Le prestataire peut étendre ce délai s'il le souhaite, mais il ne peut en tout cas pas le réduire.

Le point de départ du délai varie selon que le contrat porte sur la fourniture d'un produit ou d'un service :

- pour les produits, le délai commence à courir le lendemain du jour de leur livraison. *A fortiori*, vous pouvez renoncer au contrat avant même que le produit soit livré (p. ex., si le prestataire tarde trop à exécuter le contrat et que vous désirez renoncer au contrat pour passer commande chez un autre prestataire) ;

- pour les produits faisant l'objet de livraisons successives, le délai commence à courir le lendemain du jour de la première livraison ;

- pour les services, le délai court à partir :

  - du lendemain du jour de la conclusion du contrat,

    ou

  - du lendemain du jour où le prestataire vous a confirmé un certain nombre d'informations postérieurement à la conclusion du contrat (*supra*, n° 127) (p. ex., vous concluez un contrat de fourniture de services, qui ne sera exécuté que dans 4

mois. Un mois après la conclusion du contrat, le prestataire vous envoie la confirmation des informations requises par la loi. Dès lors, le délai de renonciation commence à courir le lendemain du jour où il vous a confirmé les informations, et non le lendemain de la conclusion du contrat). Dans ce cas, le délai ne peut en tout cas dépasser 3 mois à compter du jour de la conclusion du contrat.

Cependant, le délai de renonciation peut être prolongé à **trois mois**, à partir du lendemain de la livraison du produit ou de la conclusion du contrat de service :

- lorsque, préalablement à la conclusion du contrat, le prestataire ne vous a pas informé que vous ne bénéficiez pas d'un droit de renonciation (*supra*, n^{os} 125, 146 et 147) ;

- lorsque, postérieurement à la conclusion du contrat, le prestataire n'a pas rempli l'obligation de confirmer les informations requises par la loi (*supra*, n° 127).

Dans ce dernier cas, si les informations manquantes vous sont fournies par la suite, dans ce délai de 3 mois, le délai ordinaire de 7 jours recommence à courir. Dès lors, vous ne pourrez renoncer au contrat que dans les **7 jours** ouvrables, à partir du lendemain du jour de la réception de ces informations manquantes.

Vous devez notifier au prestataire que vous renoncez au contrat avant que le délai soit expiré.

149. Puis-je renoncer au contrat si j'ai déjà payé le prix ?

Oui. Notez qu'en principe, aucun paiement ni acompte ne peut être *exigé* de vous avant l'écoulement du délai de renonciation (*infra*, n° 155).

Néanmoins, vous êtes libre de payer immédiatement le produit ou le service si vous le désirez. Dans ce cas, si vous exercez votre droit de renonciation, le prestataire est tenu de vous rembourser les sommes versées, sans frais. Ce remboursement doit s'effectuer au plus tard dans les 30 jours de votre renonciation (*infra*, n^{os} 175 et s.).

150. Dois-je payer une indemnité pour pouvoir renoncer au contrat ?

Non. Le droit de renonciation est **gratuit** : il s'exerce sans aucune indemnité ni pénalité.

Les seuls frais qui sont à votre charge sont les frais directs exposés pour renvoyer le produit au prestataire (c'est-à-dire les frais d'expédition par voie postale).

Toutefois, vous ne devez même pas payer les frais de renvoi dans deux hypothèses :

- si le produit livré ou le service presté ne correspond pas à la description de l'offre (*infra*, n° 172) ;

- si le vendeur n'a pas rempli ses obligations d'information préalable ou postérieure à la conclusion du contrat (*supra*, n^{os} 125 et 127).

151. Puis-je renoncer à l'achat d'un produit ou d'un service si j'ai contracté un crédit pour en financer le paiement ? Que devient mon contrat de crédit en cas de renonciation ?

Oui, vous pouvez renoncer à un contrat conclu à distance même si vous avez contracté un crédit en vue de financer entièrement ou partiellement le paiement du prix du produit ou du service.

Dans ce cas, vous pouvez également renoncer au contrat de crédit, sans frais ni indemnité, si le contrat de crédit a été conclu :

- directement avec le prestataire qui fournit le produit ou le service,

ou

- avec un tiers, s'il existe entre ce tiers et le prestataire un accord en vue d'assurer le financement des produits ou services qu'il fournit.

Dans ce cas, la renonciation au contrat de crédit se fait dans les délais et selon les modalités prévus pour les contrats à distance, tels qu'expliqués aux points précédents.

152. Comment faire savoir au prestataire que je renonce au contrat ?

La loi n'impose aucune modalité particulière pour la notification de la renonciation au contrat.

Concrètement, vous pouvez notifier au prestataire votre intention de renoncer au contrat par tout moyen (simple lettre, fax ou courrier électronique).

Néanmoins, étant donné que cette renonciation doit avoir lieu endéans les délais prévus par la loi, vous seriez bien avisé de conserver une preuve de cet envoi, en cas de mauvaise foi du prestataire (qui prétendrait ne pas avoir reçu votre lettre ou votre courrier électronique, ou l'avoir reçu après l'expiration du délai).

Dès lors, mieux vaut recourir au courrier recommandé pour la notification de votre renonciation au contrat. Sachez, à cet égard, qu'il existe à présent des services de recommandé électronique, offerts par des prestataires de certification (*supra*, n° 143).

153. Quelles sont mes obligations en cas de renonciation au contrat ?

Lorsque vous décidez de renoncer au contrat, vous devez simplement le notifier au prestataire (*supra*, n° 152), et lui renvoyer le produit qu'il vous a livré (notez que le prestataire peut également vous fournir des produits en exécution d'un contrat de prestation de services).

Les frais de renvoi du produit sont à votre charge, à moins que :

- le produit livré ou le service presté ne corresponde pas à la description de l'offre ;
- le vendeur n'ait pas rempli ses obligations d'information préalable ou postérieure à la conclusion du contrat (*supra*, n^{os} 125 et 127).

154. Quelles sont les obligations du prestataire si je renonce au contrat ?

Lorsque vous exercez votre droit de renonciation, le prestataire est tenu de vous rembourser, si vous avez déjà payé le prix ou un acompte. Ce remboursement doit être effectué dans les 30 jours qui suivent votre renonciation (*infra*, n^{os} 175 et s.). Aucun frais ne peut être déduit du remboursement.

CHAPITRE V. LE PAIEMENT

155. Suis-je obligé de payer le prix avant la livraison ?

Non ! Aucun paiement ni acompte ne peut être *exigé* de vous avant l'écoulement du délai de renonciation de 7 jours (*supra*, n^{os} 144 et s.).

Cela signifie qu'en principe, le prestataire ne peut pas vous obliger à payer avant l'expiration du délai ! Il doit vous laisser le choix entre un paiement anticipé (p. ex., paiement en ligne par carte de crédit) et un paiement ultérieur (c.-à-d. après l'écoulement du délai de renonciation, p. ex., par virement bancaire dans les 15 jours de la livraison). Il ne peut en tout cas suspendre la livraison tant que vous n'avez pas payé.

Si vous bénéficiez d'un droit de renonciation, vous êtes libre de payer immédiatement ou non le produit ou le service. Sachez que si vous avez payé immédiatement, vous conservez le droit de renoncer au contrat dans le délai prévu par la loi, et que toutes les sommes que vous aurez versées vous seront remboursées (*supra*, n°149).

Par contre, si vous ne bénéficiez pas d'un droit de renonciation pour le produit ou le service que vous avez acheté (*supra*, n° 145), le prestataire peut exiger un paiement immédiat avant d'exécuter le contrat. C'est le cas, par exemple, si vous achetez des denrées périssables, un magazine ou une revue…

Or, en pratique, certains prestataires ne vous donnent pas ce choix et vous imposent un paiement anticipé… faute de quoi il est techniquement impossible de passer commande chez eux ! (p. ex., le processus de commande est uniquement programmé pour enregistrer les commandes payées anticipativement par carte de crédit, ou bien le prestataire n'exécute la commande qu'une fois qu'il a reçu votre chèque ou que votre virement a été exécuté.) Sachez qu'ils n'en ont pas le droit.

Cette attitude contraire à la loi s'explique par la crainte de certains prestataires de ne pas être payés par leurs clients. De votre côté, vous éprouvez peut-être une certaine méfiance à l'idée de payer anticipativement un prestataire inconnu, sans avoir la certitude qu'il va bel et bien exécuter la commande en retour (*infra*, n^{os} 162 et 169).

Toutefois, il ne faudrait pas sombrer dans la paranoïa et voir en tout prestataire un "arnaqueur" potentiel, prêt à empocher votre argent pour disparaître ensuite dans la nature. La grande majorité des prestataires offrant leurs services sur les réseaux mettent tout en œuvre pour faire preuve de sérieux et de fiabilité, conscients qu'il s'agit là d'une condition essentielle au développement de leur commerce.

La plupart des sites de commerce électronique contiennent des informations claires relatives aux modalités de paiement et de remboursement. En outre, de nombreux prestataires s'engagent à respecter un code de conduite dont les règles définissent une politique sérieuse en matière de paiement et de remboursement (*infra*, n^{os} 179 et s.). Souvent, le respect de ces codes est lié à l'attribution d'un label de qualité, le cas échéant sous le contrôle d'une autorité de labellisation (*infra*, n^{os} 182 et s.). Par exemple, les prestataires partenaires du système de paiement sécurisé Banxafe (*infra*, n° 159 et 163) sont labellisés par Banxafe. En cas de non respect de certains principes en matière de paiement et de remboursement, ces partenaires se voient retirer le droit d'utiliser le système Banxafe.

Outre ces initiatives privées, un arrêté royal devrait être adopté pour déterminer les critères de fiabilité auxquels les prestataires devraient se conformer pour avoir le droit d'exiger un

paiement avant l'expiration du délai de renonciation de 7 jours. L'objectif est de fixer des critères qui vous garantiront que le remboursement aura bien lieu en cas d'inexécution de la commande. Il s'agirait en quelque sorte de consacrer légalement un code de conduite ou un label de qualité, pour renforcer les initiatives privées en la matière. Néanmoins, cet arrêté royal n'a pas encore été adopté à ce jour.

156. Quels sont les moyens de paiement que je peux utiliser sur les réseaux ?

Les moyens de paiement en ligne sont très variés et diffèrent d'un prestataire à l'autre. Il est donc important de vous renseigner sur ce point avant de procéder à vos achats, afin de vérifier si vous disposez, le cas échéant, de l'équipement (logiciel et matériel) éventuellement nécessaire pour payer. Pour rappel, le prestataire a l'obligation de vous informer des modalités de paiement qui vous sont offertes, et ce, avant et après la conclusion du contrat (*supra*, n^{os} 125 et 127).

Vous trouverez dans les questions qui suivent (n^{os} 157 à 167) davantage d'explications sur les différents moyens de régler vos achats sur Internet, leurs avantages et inconvénients, ainsi que sur l'équipement éventuellement nécessaire.

157. Puis-je payer par carte de crédit ?

Il s'agit du mode de paiement le plus pratique et le plus répandu sur les réseaux. Concrètement, lorsque vous complétez le bon de commande, vous devez communiquer au vendeur le numéro et la date d'expiration de votre carte de crédit. Lorsque le vendeur reçoit votre commande, il s'adresse à l'émetteur de votre carte de crédit qui autorise le paiement après avoir vérifié si les renseignements communiqués sont exacts.

Il s'agit là d'un mode de paiement simple (il ne nécessite aucun équipement informatique particulier), rapide et admis pour la plupart des transactions internationales (vous pouvez payer dans un grand nombre de devises différentes).

De nombreuses personnes hésitent encore à payer par carte de crédit sur les réseaux, car ce système comporte certains risques (*infra*, n° 158). Cependant, des solutions techniques efficaces ont été mises en place par les émetteurs de cartes de crédit pour sécuriser les paiements sur les réseaux (*infra*, n° 159). *Les émetteurs sont d'ailleurs unanimes pour déconseiller formellement le paiement par carte sur des sites de commerce électronique non sécurisés !* En outre, d'un point de vue juridique, vous devez savoir que vous êtes entièrement protégé en cas d'usage frauduleux de votre carte de crédit (*infra*, n° 160).

158. Quels sont les risques liés à l'utilisation d'une carte de crédit sur les réseaux ?

Vous hésitez peut-être à utiliser votre carte de crédit sur les réseaux, en raison des spectaculaires affaires de *hacking* et de fraudes largement relayées par la presse. Il convient de dédramatiser quelque peu la situation. En effet, il existe aujourd'hui des techniques et des parades permettant de garantir un degré élevé de sécurité pour les paiements en ligne. Néanmoins, il est vrai qu'en matière de sécurité sur les réseaux, le risque zéro n'existe pas.

Le premier problème lié au paiement par carte de crédit est que la connaissance du numéro de votre carte et de sa date d'expiration suffit pour effectuer des achats à vos frais. En effet, pour payer par carte de crédit, il n'est pas nécessaire de s'identifier comme titulaire de la carte ni d'introduire un code secret. Il ne faudrait donc pas que ces données

tombent aux mains de tiers. Il est donc important de veiller à ce que la transmission de ces données soit protégée par des dispositifs techniques (*infra*, n° 159).

En outre, certains prestataires conservent ces informations dans des bases de données, en particulier si vous vous enregistrez comme client auprès de leur site. Ce système présente l'avantage de vous offrir un certain confort, car vous n'avez pas à réintroduire toutes vos données personnelles à chaque commande. On peut craindre, par contre, que ces informations ne soient obtenues par un *hacker* (*supra*, n^{os} 104 et s.) qui réussirait à s'introduire dans la base de donnée du prestataire. Il faut donc que cette base de données soit protégée par des systèmes de sécurité. Informez-vous sur le site du prestataire à propos de la durée de conservation de vos données bancaires et de l'existence d'un système de sécurité protégeant la base de données contre tout accès frauduleux. Certains prestataires, afin d'éviter ce problème, ne conservent jamais ces données plus de temps qu'il n'est nécessaire pour enregistrer votre paiement.

Enfin, il existe un risque de fraude de la part du prestataire lui-même, qui prélèverait, grâce à vos données bancaires, un montant supérieur au montant de vos achats, ou utiliserait ces données pour prélever plusieurs paiements en sa faveur. Toutefois, ce risque est inhérent à l'utilisation de toute carte de crédit, même en dehors des réseaux (le même risque existe lorsque vous transmettez ces données par téléphone ou par fax). En outre, tout prestataire établi en Europe a désormais l'obligation de fournir sur son site un certain nombre d'informations relatives à son identité et à son activité professionnelle, et il ne peut disparaître dans la nature aussi facilement (*supra*, n° 122). Enfin, de nombreux prestataires adhèrent à des codes de conduite ou font labelliser leur site afin de vous fournir une garantie de leur sérieux et de leur fiabilité (*infra*, n^{os} 179 et s.).

En l'absence de système de sécurité mis en place sur le site du prestataire ou face à un prestataire qui ne s'est pas identifié correctement, il est formellement déconseillé d'effectuer vos paiements par carte de crédit sur le site. Dès lors, si vous désirez payer vos achats par carte de crédit, informez-vous d'abord des mesures de sécurité prises par le prestataire pour éviter les usages frauduleux de votre carte.

159. Quels sont les dispositifs techniques mis en place sur les réseaux pour sécuriser les paiements par carte de crédit ?

Il existe différents systèmes afin de sécuriser les paiements par cartes de crédit sur les réseaux. Si vous désirez payer vos achats par carte de crédit, informez-vous d'abord des mesures de sécurité prises par le prestataire pour éviter les usages frauduleux de votre carte ! En l'absence de système de sécurité mis en place sur le site du prestataire, il est déconseillé d'effectuer vos paiements par carte de crédit sur le site. En effet, un prestataire qui s'abstiendrait de prendre des mesures techniques pour sécuriser vos paiements ne ferait guère la preuve de son sérieux et de sa fiabilité !

Il existe principalement deux standards de sécurisation des paiements sur les réseaux : le SSL et le SET. En Belgique, ces techniques sont notamment appliquées dans le cadre d'un nouveau système de paiement sécurisé appelé Banxafe, qui est brièvement présenté ci-dessous.

SSL (Secure Sockets Layer)

Il s'agit d'un protocole assurant la confidentialité et l'intégrité de données transmises sur les réseaux, en les cryptant (à l'aide d'une signature digitale). Ce système efficace est extrêmement répandu et utilisé par une large majorité de prestataires sérieux et fiables. Vous pourrez facilement trouver sur leur site une information claire à cet égard.

De votre côté, vous n'avez aucune démarche particulière à faire pour sécuriser la transmission de vos données bancaires, étant donné que le système de protection est aujourd'hui intégré aux logiciels de navigation Netscape et Internet Explorer. Tout se fait automatiquement. Vous êtes averti que la transmission est bien sécurisée par l'apparition d'un petit cadenas fermé dans le coin inférieur droit de votre fenêtre de navigation et par le fait que l'adresse URL commence par "https".

Grâce à ce standard, vos données bancaires – numéro de carte et date d'expiration – circulent de manière cryptée sur les réseaux. Ainsi, seul le prestataire aura accès à ces données. Si elles venaient à être interceptées par un tiers au cours de la transmission, ce dernier ne pourrait les déchiffrer. Ce système assure la confidentialité dans le transfert des données bancaires sur les réseaux mais ne résout pas le problème de la conservation de vos données bancaires par le prestataire.

SET (Secure Electronic Transaction)

Il s'agit d'un standard spécifiquement destiné à sécuriser les paiements par carte sur les réseaux qui s'avère en outre plus sûr que le SSL car le prestataire n'a pas accès à vos données bancaires. En effet, celles-ci sont directement envoyées sous forme cryptée à votre émetteur de carte de crédit qui est le seul à pouvoir les déchiffrer pour vérifier la validité de la transaction. Cela évite ainsi tout risque de *hacking* (voire de malhonnêteté du prestataire lui-même) lié au stockage par le prestataire de vos données bancaires dans une base de données. Enfin, votre vie privée est respectée étant donné que votre émetteur de carte n'a pas la possibilité d'accéder aux détails de votre commande.

Le standard SET permet également votre identification sur les réseaux (ainsi que celle du prestataire) grâce à un certificat. Ainsi, personne d'autre que vous ne peut payer avec votre carte de crédit.

Une application concrète en Belgique : Banxafe

Banksys a développé un système de paiement sécurisé en collaboration avec la BCC (*Bank Card Company*, c'est-à-dire Visa et MasterCard) et les banques belges (Bacob, BBL, Dexia, Fortis et KBC). Ce système, appelé Banxafe, permet de payer en ligne avec sa carte de crédit de manière totalement sécurisée. Ce système est aussi utilisé avec un lecteur de carte à puce pour les paiements sur Internet avec carte de débit Bancontact/Mister Cash (*infra*, n° 163).

Le système est très facile à utiliser et ne nécessite l'installation d'aucun logiciel sur votre ordinateur. Ce mode de paiement est proposé sur les sites belges affiliés à Banxafe (dont la liste figure sur le site www.banxafe.be) et équipés du système adéquat. Il fonctionne également sur tous les sites étrangers utilisant les standards SSL et SET (les logos "SET" ou "MasterCard SET" doivent apparaître sur le site au moment de payer) ou le standard 3D Secure.

Concrètement, en choisissant le paiement sécurisé par Banxafe, vous cliquez sur un hyperlien qui vous envoie vers le site de Banksys. Dès lors, vous n'introduisez plus vos données bancaires (numéro de carte, date d'expiration et type de carte) sur le site du prestataire mais sur le serveur sécurisé de Banksys. Ainsi, ni le prestataire, ni un éventuel *hacker*, ne peuvent accéder à vos données. Ensuite, Banksys confirme au prestataire que votre paiement a été valablement enregistré.
Pour plus de détails sur ce nouveau mode de paiement, surfez sur www.banxafe.be et www.mybanxafe.be.

160. Dois-je supporter les conséquences si quelqu'un utilise ma carte de crédit frauduleusement sur les réseaux ?

Non !

La plupart des gens pensent à tort qu'ils devront supporter les conséquences financières en cas d'utilisation frauduleuse de leur carte de crédit. C'est faux ! Dans une telle hypothèse, vous êtes protégé par la loi qui prévoit que c'est à l'émetteur de la carte de crédit – et non à vous ! –, qu'il revient d'assumer les conséquences d'une telle fraude.

La loi précise en effet que vous n'êtes pas responsable, c'est-à-dire que vous ne devez pas supporter cette perte, si votre carte de crédit a été utilisée à votre insu, à distance (c-à-d. sans présentation physique de la carte : sur les réseaux, par téléphone, fax...) et sans identification électronique (c'est-à-dire sans recourir à un dispositif de signature électronique ou autre système de sécurité). La seule utilisation d'un code confidentiel, sans autre procédé d'identification électronique (sans signature digitale) ne suffit pas à engager votre responsabilité.

En d'autres termes, dans ces circonstances, si quelqu'un utilise frauduleusement votre numéro de carte de crédit et sa date d'expiration pour effectuer des achats sur les réseaux, vous ne devrez pas en subir les conséquences financières. A moins, bien entendu, que vous ayez agi frauduleusement (p. ex., si vous avez donné à un tiers votre carte de crédit, puis notifié à l'émetteur la perte ou le vol de votre carte ; ou bien si vous avez utilisé vous-même votre carte après avoir prétendu à l'émetteur qu'elle avait été perdue ou volée).

Dès lors, vous pouvez demander l'annulation du paiement effectué suite à des opérations frauduleuses (*infra*, n° 161). L'émetteur a l'obligation de vous rembourser dans les plus brefs délais tous les montants qui vous auront été débités dans ces circonstances.

L'objectif du législateur est d'obliger les émetteurs de cartes de crédit à mettre en place des systèmes assurant une utilisation sécurisée des cartes de crédit sur les réseaux. La méthode s'avère efficace étant donné que ces dernières années, de grands progrès techniques ont été faits, sous l'impulsion des émetteurs de cartes de crédit, en vue de protéger la transmission de vos données bancaires (*supra*, n° 159).

161. Que faire si je constate que quelqu'un utilise ma carte de crédit frauduleusement ?

Si vous vous rendez compte du vol ou de la perte de votre carte de crédit, vous devez immédiatement en avertir l'émetteur de votre carte. Ce dernier est tenu de mettre à votre disposition, 24 heures sur 24, un numéro de téléphone à cet effet (p. ex., le numéro Card Stop de la BCC, pour Visa et MasterCard : 070 344.344).

De même, si vous repérez, dans le relevé des opérations effectuées avec votre carte, des erreurs, des irrégularités ou des opérations effectuées sans votre accord, avertissez-en immédiatement votre émetteur. Celui-ci met également un numéro à votre disposition pour lui signaler tout usage frauduleux de votre carte (BCC permet les notifications par téléphone au 02 205.87.87 ou par fax au 02 205.81.08). Après une rapide enquête, il vous remboursera les sommes indûment perçues, dans les plus brefs délais.

162. Que faire si le prestataire n'exécute pas le contrat alors que j'ai payé anticipativement par carte de crédit ?

Si vous avez payé anticipativement par carte de crédit et que le prestataire tarde à exécuter votre commande, pas de panique ! Prenez d'abord contact avec lui pour obtenir des explications (*infra*, n° 169).

S'il ne vous répond pas ou fait manifestement preuve de mauvaise volonté pour vous rembourser, vous pouvez également prendre contact avec votre émetteur de carte de crédit. Ce dernier met peut-être à votre disposition un service vous permettant d'introduire auprès de lui une procédure de contestation en cas de non exécution du contrat pour lequel vous avez été débité. Néanmoins, sachez que la loi n'oblige pas l'émetteur à vous fournir un tel service. En effet, votre émetteur de carte de crédit n'est qu'un intermédiaire de paiement et il n'a pas à intervenir dans vos transactions en cas d'absence ou de retard de livraison, encore moins en cas de livraison non conforme. Renseignez-vous donc auprès de lui à ce sujet pour voir les solutions qu'il propose.

Souvent, les émetteurs de carte de crédit ont prévu une procédure de contestation. Dans cette hypothèse, veillez à bien communiquer tous les détails de l'opération que vous contestez. Ainsi, une copie du document reprenant l'état détaillé de vos dépenses, que l'émetteur vous envoie périodiquement (souvent tous les mois) et sur lequel vous aurez indiqué l'opération contestée, peut s'avérer bien utile. Il convient également de communiquer tous les éléments de preuve dont vous disposez (courrier échangé avec le prestataire, p. ex.). A cet égard, l'accusé de réception de la commande que le prestataire a l'obligation de vous envoyer (*supra*, n° 127) constitue un élément important. A la réception de votre contestation, l'émetteur de votre carte de crédit prendra lui-même contact avec le prestataire afin de lui demander des explications.

163. Puis-je payer avec ma carte de débit Bancontact / Mister Cash ?

Il est possible, sur certains sites, de payer avec votre carte de débit (Bancontact/MisterCash), grâce au système Banxafe développé par Banksys (*supra*, n° 159).

Pour pouvoir payer par carte de débit sur Internet, vous devez disposer d'un lecteur de carte (un boîtier muni d'un écran et d'un clavier dans lequel on peut insérer sa carte à puce) connecté à votre ordinateur. Ce lecteur (le C-ZAM/PC) peut être acheté auprès de votre banque (pour 19 euros) ou dans certains magasins (dont la liste figure sur le site www.banxafe.be, pour environ 50 euros dans une version plus élaborée). Vous devez également installer sur votre ordinateur un logiciel appelé "portefeuille électronique" (le *banxafe wallet*, fourni avec le lecteur de carte, sur le CD-ROM d'installation).

Le dispositif fonctionne comme dans un magasin traditionnel : une fois vos articles sélectionnés, vous optez pour le paiement par Bancontact et le serveur du prestataire transmet à votre ordinateur toutes les informations nécessaires au paiement (produit, prix…). Vous devez alors une première fois introduire le code secret de votre carte au moyen du clavier du lecteur, pour vous identifier. Le montant de vos achats apparaît alors sur le lecteur de carte et il ne vous reste plus qu'à valider ce montant en introduisant une seconde fois votre code secret. En aucun cas votre code secret ne transite sur les réseaux ! Il ne sort même pas du lecteur.

Grâce au lecteur de carte, il vous est également possible de recharger votre carte Proton en ligne. Par contre, les paiements par Proton ne sont pas possibles sur Internet.

Pour plus de détails sur ce mode de paiement, surfez sur www.banxafe.be et www.mybanxafe.be.

164. Puis-je payer directement sur le site par virement électronique ?

Certains prestataires vous offrent parfois la possibilité de régler vos achats par virement électronique, directement sur leur site. Ce système se différencie du paiement par virement classique (sur papier, par *self-banking*, *phone banking* ou *home-banking*), en ce sens que le paiement s'effectue en quelques minutes, au lieu de plusieurs jours.

Pour utiliser ce mode de paiement, vous devez d'abord être équipé d'un système de *home-banking* fourni par votre banque. Tous les logiciels de *home-banking* permettent de faire des virements à domicile, par voie électronique, de la même manière que dans les appareils de *self-banking*. Par contre, tous ne permettent pas de payer *directement sur un site web* par virement électronique. Pour cela, il faut en outre que votre banque vous fournisse un tel service. A titre d'exemple, la BBL offre actuellement cette possibilité, via un service appelé Home'Pay (www.bbl.be/homebank/fr et www.bblshoppingmall.be).

En outre, vous ne pouvez utiliser ce mode de paiement qu'auprès des prestataires ayant passé un accord avec votre banque pour créer une passerelle entre leur site de commerce électronique et la plate-forme de *home-banking* de celle-ci.

Concrètement, si le site visité vous permet de régler vos achats par ce mode de paiement et que vous disposez de l'équipement nécessaire, la procédure se déroule comme suit. Lorsque vous choisissez de payer par virement électronique sur le site, vous cliquez sur un lien qui vous envoie directement sur la plate-forme de *home-banking* de votre institution bancaire sur laquelle vous attend un virement déjà complété à l'ordre du prestataire. Il ne vous reste plus qu'à valider ce virement au moyen d'un code confidentiel. Votre banque informe alors le prestataire que votre paiement est en cours.

Ce système est à la fois simple et sûr, puisque vous communiquez directement avec votre organisme bancaire, sur une plate-forme de *home-banking* sécurisée, sans que vos données bancaires circulent sur les réseaux. Cependant, à l'heure actuelle, un tel système est limité au niveau national, entre banques et prestataires d'un même pays.

165. Puis-je payer par virement bancaire ?

Il est parfois également possible de régler vos achats par virement bancaire ordinaire (sur papier, par *self-banking*, *phone banking* ou *home-banking* classique, à ne pas confondre avec le virement électronique directement sur le site : *supra*, n° 164). Veillez, dès lors, à bien indiquer le numéro de référence de la commande dans la communication.

Certains sites vous permettent de payer par virement après réception de la commande, ce qui est extrêmement pratique. Cependant, craignant les mauvais payeurs, de nombreux sites n'autorisent le virement que pour un paiement anticipé. Dans cette dernière hypothèse, ce n'est qu'à la réception et à l'enregistrement de votre paiement que la commande vous sera livrée, ce qui peut allonger les délais de livraison. En outre, cette formule n'est guère avantageuse pour les achats transfrontaliers, vu les importants frais bancaires liés aux virements internationaux.

166. Puis-je payer par chèque ?

Certains prestataires vous permettent de régler vos achats par chèque bancaire, envoyé par La Poste. Si vous avez choisi ce mode de paiement, les informations pratiques

relatives au paiement (mentions à inscrire sur le chèque, adresse d'expédition du chèque, conditions d'acceptation…) vous seront communiquées après la commande, par l'affichage d'une page web et/ou dans un courrier électronique confirmant l'enregistrement de votre commande.

Cette formule peut s'avérer pratique si vous ne désirez pas régler vos achats par un paiement en ligne. Néanmoins, elle est limitée à l'échelon national, étant donné que les eurochèques ne sont généralement plus acceptés par les commerçants (en effet, depuis le 1er janvier 2002, les eurochèques ne sont plus garantis). En outre, si le paiement par chèque est proposé par le prestataire comme mode de paiement anticipé, le délai de livraison sera allongé, étant donné que le prestataire attendra d'avoir reçu le paiement avant d'expédier la commande.

167. Puis-je payer à la livraison ?

Certains prestataires vous offrent la possibilité de payer le produit à la livraison. Vous pouvez ainsi payer directement au livreur à domicile (en espèces, par chèque ou, le cas échéant, par chèques repas ou par carte de crédit). Parfois, vous devez prendre livraison de votre commande vous-même dans un point d'enlèvement (station essence, supermarché…), où vous pourrez payer vos achats à la caisse. Cette formule est fréquemment utilisée dans le secteur alimentaire (supermarché en ligne, traiteur à domicile, livreur de pizzas, etc.).

Le paiement à la livraison peut être pratique si vous ne disposez d'aucun autre moyen de paiement ou si vous n'avez pas envie d'utiliser votre carte de crédit sur les réseaux, malgré les protections techniques et juridiques existantes (*supra*, nos 159 et s.).

Néanmoins, le système est loin d'être généralisé sur les réseaux et ne peut être mis en œuvre pour la vente internationale, pour des raisons pratiques évidentes. En outre, le recours à cette formule entraîne souvent un coût supplémentaire qui vous est facturé. Il faut que vous soyez présent au moment de la livraison ou que vous vous déplaciez pour prendre livraison de votre commande.

CHAPITRE VI. LA LIVRAISON DU PRODUIT OU LA PRESTATION DU SERVICE

168. Quand le prestataire doit-il exécuter le contrat ?

Le prestataire est tenu d'exécuter la commande dans un délai de maximum 30 jours, à partir du lendemain de la transmission de votre commande.

Vous pouvez également convenir avec lui d'un autre délai, le cas échéant supérieur à 30 jours.

169. Que faire si le prestataire tarde à exécuter la commande ?

Lorsque le prestataire tarde à exécuter la commande et vous laisse sans nouvelles, pas de panique ! Le mieux est de prendre contact avec lui pour obtenir des explications. Il se peut qu'il ait à faire face à des difficultés de stock et que le produit que vous avez commandé soit momentanément indisponible. A moins que le produit ne se soit égaré lors de l'expédition, auquel cas c'est au prestataire à en assumer l'entière responsabilité (*infra*, n° 171).

Si, au terme du délai légal de 30 jours (ou du délai convenu avec vous), le prestataire n'a pas encore exécuté votre commande, le contrat est résolu de plein droit. Cela signifie que vous ne serez plus lié par le contrat si le délai d'exécution est passé (à moins que le prestataire n'ait pu s'exécuter en raison d'un cas de force majeure). Aucun frais ni aucune indemnité ne pourra vous être réclamé suite à la résolution du contrat. En outre, si vous aviez déjà versé un acompte ou payé la totalité du prix, le prestataire devra vous rembourser l'intégralité de ces sommes dans les 30 jours (*infra*, n^{os} 175 et s.). Enfin, vous pourrez éventuellement lui réclamer des dommages et intérêts, si cette inexécution vous a causé un dommage.

Vous pouvez toutefois, si vous le désirez, convenir avec le prestataire de la prolongation du délai.

Notez encore que vous n'êtes pas obligé d'attendre l'expiration du délai de 30 jours pour mettre fin au contrat : vous pouvez également exercer votre droit de renonciation avant même la livraison du produit ou dans les 7 jours ouvrables de la conclusion du contrat de service (*supra*, n^{os} 144 et s., spéc. n° 148).

170. Le contrat s'exécute-t-il en ligne ou hors ligne ?

Si la commande porte sur un produit ou un service immatériel (logiciel, vidéo ou film à la demande, consultation d'un service d'information…), le contrat sera également exécuté, de façon instantanée, par le biais des réseaux, par téléchargement.

Si la commande porte sur un bien matériel (livre, vêtement, appareil électroménager…) ou un service qui se matérialise par la fourniture d'un produit (abonnement à un périodique sur support papier…), elle sera exécutée par l'intermédiaire des modes de transport traditionnels (paquet ou pli postal acheminé par avion, train, bateau, transport routier…).

Les contrats peuvent donc être soit conclus et exécutés via les réseaux, soit seulement conclus par leur biais, mais exécutés en dehors de ceux-ci.

171. Dois-je payer le prix si le produit s'égare ou est abîmé lors de la livraison ?

Non. L'envoi de produits ou de titres représentatifs de services se fait toujours aux risques et périls du prestataire.

Dès lors, aucun paiement ne peut être exigé de vous si le produit n'arrive jamais. Si vous avez déjà payé le prix ou un acompte, ces sommes doivent vous être remboursées (*infra*, n° 175).

Si le produit arrive en mauvais état, c'est au prestataire à en supporter les conséquences. En pratique, vous pouvez garder le produit et demandez au prestataire une réduction du prix. Vous pouvez également renvoyer le produit au prestataire qui vous en livrera un nouveau en parfait état.

172. Que faire si le produit livré ne correspond pas à la description qui en était faite sur le site ?

Vous pouvez renoncer au contrat, dans les 7 jours ouvrables à partir du lendemain de la livraison, et renvoyer le produit non conforme au prestataire (*supra*, n^{os} 144 et s.). Dans ce cas, les frais de renvoi sont à charge du prestataire (*supra*, n° 150).

173. Quelles informations suis-je en droit de recevoir lors de la livraison ?

Le prestataire doit vous fournir un certain nombre d'informations postérieurement à la conclusion du contrat et en tout cas au plus tard au moment de la livraison des produits (*supra*, n° 127).

Ces informations sont les suivantes :

- l'identité et l'adresse géographique du vendeur ;
- le prix du produit ou du service ;
- les frais de livraison, le cas échéant ;
- les modalités de paiement, de livraison ou d'exécution du contrat ;
- la durée de validité de l'offre ou du prix ;
- dans le cas de fourniture durable ou périodique d'un produit ou d'un service, la durée minimale du contrat ;
- l'adresse géographique où vous pourrez adresser une plainte ;
- les informations relatives aux services après-vente et aux garanties commerciales existants ;
- dans le cadre d'un contrat à durée indéterminée ou d'une durée supérieure à 1 an, les conditions dans lesquelles vous pouvez résilier le contrat ;
- l'existence ou l'absence d'un droit de renonciation (*supra*, n° 144) et les modalités et conditions d'exercice de ce droit.

A cet égard, l'une des deux clauses suivantes, rédigée en caractères gras, dans un cadre distinct du reste du texte, doit figurer en première page du document, ou en tout cas de manière bien visible :

- (si vous avez un droit de renonciation) "Le consommateur a le droit de notifier au vendeur qu'il renonce à l'achat, sans pénalités et sans indication du motif, dans les … jours ouvrables (au minimum 7 jours) à dater du lendemain du jour de la livraison du produit ou de la conclusion du contrat de service" ;

- (si vous n'avez pas de droit de renonciation) "Le consommateur ne dispose pas du droit de renoncer à l'achat".

Si le prestataire vous a fourni ces informations auparavant (p. ex. par courrier électronique), elles ne doivent plus vous être fournies à la livraison.

174. Quelles sont les conséquences de la livraison ?

La livraison fait courir le délai dans lequel vous pouvez renoncer au contrat. En effet, à partir du lendemain de la livraison, vous disposez de 7 jours ouvrables pour notifier au prestataire que vous renoncez au contrat (*supra*, n° 148).

CHAPITRE VII. LE REMBOURSEMENT ET LE SERVICE APRES-VENTE

175. Dans quels cas puis-je demander le remboursement de mes achats ?

Vous pouvez réclamer au prestataire de vous rembourser dans deux hypothèses :

- lorsque vous exercez votre droit de renonciation (*supra*, n° 149, 150 et 154) ;
- lorsque le contrat n'a pas été exécuté (*supra*, n° 169).

Vous avez alors droit au remboursement des sommes que vous avez déjà versées, qu'il s'agisse de l'intégralité du prix ou d'un acompte. Aucun frais et aucune indemnité ne peuvent être retenus par le prestataire.

176. Quelles sont les formalités à accomplir pour obtenir le remboursement ?

Il convient de prendre contact avec le prestataire pour lui signaler que vous désirez être remboursé des sommes que vous lui avez versées. Rappelez-lui toutes les données relatives à votre commande ainsi que les montants versés. Veillez à conserver une preuve de paiement pour la lui montrer en cas de contestation.

La demande de remboursement ne doit revêtir aucune forme particulière. Elle peut être faite par téléphone, fax, courrier électronique ou simple lettre. Néanmoins, il est plus prudent de recourir à la lettre recommandée à la Poste ou au recommandé électronique, afin de vous ménager une preuve de votre demande.

Si vous avez payé par carte de crédit, prenez contact avec l'émetteur de votre carte qui met peut-être à votre disposition un service vous permettant d'introduire auprès de lui une procédure de contestation en cas de non exécution du contrat pour lequel vous avez été débité (*supra*, n° 162).

177. Si je renonce au contrat, dans quel délai le prestataire doit-il me rembourser ?

Si vous renoncez au contrat, le remboursement doit avoir lieu dans les 30 jours qui suivent la renonciation.

Si le contrat n'est pas exécuté dans les 30 jours de la transmission de votre commande, il est résolu de plein droit et le remboursement doit avoir lieu dans les 30 jours de la résolution. Cela signifie qu'il ne peut s'écouler plus de 60 jours entre votre commande (non exécutée) et le remboursement.

178. Les produits et services achetés sur Internet sont-ils couverts par une garantie ou un service après-vente ?

Oui, comme pour les achats dans les magasins traditionnels, vos achats peuvent être couverts par une garantie et, le cas échéant, un service après-vente.

A cet égard, le prestataire a l'obligation de vous fournir les informations relatives aux garanties commerciales existantes et au service après-vente. Cette information doit vous être fournie postérieurement à la conclusion du contrat (*supra*, n° 127).

CHAPITRE VIII. LES CODES DE CONDUITE ET LA LABELLISATION

179. Qu'est-ce qu'un code de conduite ?

Tantôt inquiets des carences et du déficit de légitimité dont peuvent souffrir les nouvelles cyber-activités du fait de pratiques illicites non réprimées, tantôt soucieux de créer la confiance et de rassurer les consommateurs, les différents acteurs d'Internet n'ont pas tardé à tirer parti des potentialités du réseau pour investir spontanément ce nouveau champ économique et communicationnel et pour y mettre en œuvre différents moyens "privés" de régulation.

De manière générale, les codes de conduite répondent au souci d'assurer une cohésion entre les acteurs d'une communauté ou d'un secteur déterminé, en instaurant des "règles du jeu" qui présideront à une régulation équilibrée des acteurs en présence. Plus concrètement, le code de conduite peut être défini comme un corps de règles élaborées par un organisme et qui, tout en n'ayant pas un caractère directement obligatoire, a pour but d'encadrer et d'orienter les comportements.

Face à un phénomène "transfrontières" , fluide, polymorphe, ambigu, tel qu'Internet, des entreprises, des associations et des organismes s'engagent ainsi à influencer ou à réglementer les pratiques commerciales pour leur propre bien et pour celui de leur collectivité. Ces codes de conduite apparaissent dans différents domaines d'activités (publicité, marketing direct, etc.) et visent différents thèmes (protection des consommateurs, des mineurs, de la vie privée, etc.). Ils présentent un intérêt pratique dans la mesure où ils édictent une série de mesures auto-régulatrices, complémentaires aux lois existantes, destinées à garantir de la part des entreprises visées des comportements loyaux et honnêtes.

Lorsqu'un site web adhère à un code de conduite, il entend généralement le faire savoir. Le site va donc souvent mettre en évidence cet élément par l'affichage d'une icône, d'un label ou d'un lien hypertexte qui peuvent renvoyer à ce code de conduite. Il est également possible que le site fasse mention de ce code de conduite dans ses conditions générales.

180. Puis-je me fier à un code de conduite ?

Les codes de conduite dans les environnements numériques se caractérisent par une grande hétérogénéité en ce qui concerne tant leurs auteurs, leur contenu que leurs destinataires. Un site doté d'un code de conduite n'est pas nécessairement un gage de fiabilité.

De manière générale, vous ne devez pas perdre de vue que l'élaboration d'un code conduite n'est pas seulement le résultat d'une responsabilisation "éthique" des acteurs d'une communauté. En effet, le code de conduite constitue un argument commercial indéniable, une sorte de "vitrine" visant à valoriser une profession, un secteur ou un groupement aux yeux de l'opinion publique.

En conséquence, vous devez rester vigilants car la qualité des codes de conduite est très variable… Pour vous aider à évaluer la fiabilité de certains codes de conduite, vous pouvez notamment consulter le *e-confidence forum*, initiative de l'Union européenne, à l'adresse http://econfidence.jrc.it.

181. Puis-je me prévaloir d'un code de conduite ?

La portée juridique d'un code de conduite n'est pas évidente à déterminer. En effet, nombre de codes de bonne conduite, d'éthique, de déontologie apparaissent *a priori* comme des documents à caractère exclusivement incitatif, contenant de simples recommandations. Ils ne disposent donc pas *a priori* d'une légitimité et d'une force juridique équivalentes aux lois et réglementations étatiques.

Certains codes de conduite prévoient la possibilité pour un tiers (utilisateur ou autre) d'introduire une plainte auprès de l'association concernée pour non respect du code par l'un de ses membres. Généralement, une procédure est mise en place et des sanctions sont prévues. Cela constitue un premier type de recours possible.

On peut aussi envisager qu'un utilisateur se prévale des dispositions d'un code de conduite lors d'un recours en justice, indépendamment de toute intervention de l'association. Pour cela, il faut cependant que le professionnel avec lequel vous contractez fasse expressément référence, dans l'un ou l'autre document qu'il transmet, au respect du code de conduite. Le code devient à ce moment l'un des éléments du contrat, inclus par référence, dont l'utilisateur peut se prévaloir (cela pourrait être le cas si le vendeur fait une référence sur son site au code de conduite et y renvoie par hyperlien).

Par contre, si aucune référence au code de conduite n'est faite dans les documents contractuels, il n'est pas certain que le code ait valeur obligatoire et que vous puissiez l'invoquer pour appuyer votre demande en justice.

182. Qu'est-ce que la labellisation ?

La labellisation est une technique consistant à afficher un label – ou étiquette – sur un site web afin de mettre en évidence l'engagement de ce site à respecter certains critères. Elle a pour but d'accroître la confiance des consommateurs en leur offrant davantage de transparence et de garanties quant au respect par les sites web de normes et critères prédéfinis.

Concrètement, en visitant un site web, vous trouverez peut-être un label qui est soit apposé par le site lui-même, soit par une société tierce. Si vous cliquez sur le label, les règles relatives à son fonctionnement devraient s'afficher à l'écran de manière à vous permettre de vérifier les engagements auxquels le site a souscrit.

Il importe d'attirer l'attention sur le fait que la labellisation n'a de sens que si elle apporte un élément supplémentaire au simple respect de la législation. Le rôle du label n'est donc pas seulement d'affirmer le respect de la législation mais d'apporter une valeur ajoutée aux exigences réglementaires qui s'imposent à tous. C'est à ce prix qu'il peut alors constituer un véritable "sceau de qualité".

183. Puis-je me fier à un label affiché sur un site web ?

Attention ! Le simple affichage d'un label sur un site ne suffit pas pour attester la qualité et la fiabilité du site. En effet, vous ne devez pas vous fier uniquement à la présence d'un label pour réaliser des achats "les yeux fermés".

Divers éléments doivent vous permettre de vous éclairer sur la fiabilité de l'initiative de labellisation.

Vous devez d'abord avoir le réflexe de cliquer sur le label (ou l'hyperlien offert sur le site) afin de vérifier ce qu'il signifie exactement. L'hyperlien doit logiquement vous amener à une page qui fournit toutes les informations utiles relatives au label.

Il est important ensuite que vous sachiez qui est à l'origine du label, et par là, quels contrôles sont exercés. La labellisation peut être, en effet, interne ou externe selon qu'elle implique ou non l'intervention d'un ou de plusieurs organismes tiers dans le contrôle du respect de critères prédéfinis. Une labellisation de nature externe offre plus de garanties, soit qu'un contrôle aléatoire *a posteriori* est effectué quant au respect des critères prédéfinis, soit, à l'inverse, que le label est accordé sur la base d'un contrôle *a priori* du site web.

Dans cette optique, l'association des consommateurs Test Achats a pris l'initiative de mettre sur pied un système de labellisation, le *Web Trader*, basé sur un code de conduite. Ce système de labellisation a pour objectif de développer davantage le commerce électronique en certifiant la fiabilité et le sérieux des sites web affichant le logo. Le consommateur visitant de tels sites a donc l'assurance que ceux-ci respectent le code *Web Trader* (voy. http://www.budget-net.com/webtradersite/webtrader_home_be.html). Une initiative parallèle de labellisation a aussi été lancée par le réseau des Chambres de Commerce et d'Industrie de Belgique (voy. http://www.chamber-trust.be/fr/label-qui.html).

CHAPITRE IX. LES MODES ALTERNATIFS DE RESOLUTION DES LITIGES EN LIGNE

184. Qu'est-ce qu'un mode alternatif de résolution des litiges en ligne (ADR) ?

Internet est un lieu d'interactions dans lequel naissent inévitablement des conflits. Ceux-ci peuvent être très divers. A côté des litiges qui peuvent surgir dans le cadre d'une relation contractuelle, apparaissent de nouvelles formes de litiges propres aux réseaux. Par ailleurs, les réseaux se jouant des frontières, les parties à un litige sont souvent domiciliées ou établies dans des pays fort éloignés. Cette dimension internationale accentue encore la complexité des litiges.

Face à un tel phénomène, certains acteurs mettent en place des mécanismes de résolution des conflits qui se distinguent des voies judiciaires traditionnelles (cours et tribunaux).

Ces mécanismes alternatifs de résolution des conflits ou ADR (*Alternative Dispute Resolution*) peuvent prendre la forme d'une médiation, d'une conciliation, d'un arbitrage ou encore d'une procédure hybride. L'objectif est de s'adresser à une personne qui va se charger de trouver une solution au conflit ou, à tout le moins, d'aider les parties à trouver une solution au conflit.

Depuis peu, certains organismes permettent de recourir à ce genre de mécanisme directement sur Internet. Bien entendu, certains sites proposent de régler, en interne, les plaintes qui leur parviennent en vous offrant l'opportunité d'exprimer vos griefs auprès d'une "hotline". Ils s'engagent alors à régler le différend avec vous. Toutefois, il est préférable de se tourner vers des sites proposant le recours à un organisme tiers chargé de résoudre les conflits en ligne. Cette deuxième solution offre plus de garanties puisqu'un tiers neutre intervient dans la résolution du litige entre les parties.

Si l'on décide d'avoir recours à un tiers pour la résolution d'un litige, plusieurs cas de figure peuvent se présenter. Si vous optez pour un mécanisme de médiation ou de conciliation, vous allez confier le conflit à un tiers neutre qui va tenter d'établir une communication entre vous et la société ou la personne avec laquelle vous êtes en conflit afin de parvenir à un accord. Si vous choisissez d'avoir recours à l'arbitrage, vous allez alors confier le conflit à un tiers neutre, *l'arbitre*, qui va décider quelle solution doit être adoptée. A la différence de la conciliation et de la médiation, les parties en conflit doivent se soumettre à la décision de l'arbitre.

185. Quand et comment recourir à ce type de mécanisme ?

Ces procédures de règlement des litiges constituent une réponse appropriée et efficace aux petits litiges. En effet, ces procédures offrent une voie alternative pour la résolution de litiges portant sur des opérations d'un faible montant, pour lesquelles une action en justice classique se révélerait trop onéreuse.

Pour recourir à ce type de procédures, il vous suffit d'accéder aux sites qui offrent un tel service et de remplir un formulaire en ligne (voy., par exemple, http://www.ecodir.org).

Pour pouvoir recourir à une procédure alternative de résolution de litige, vous devez cependant avoir l'accord de la personne avec laquelle vous êtes en conflit. Soit cette dernière a déclaré sur son site ou par courrier qu'elle accepte de recourir à la médiation ou à l'arbitrage et elle est alors obligée d'y recourir si vous en faites la demande. Soit elle ne

s'est engagée à rien préalablement mais elle accepte la procédure de médiation et d'arbitrage.

Sachez également qu'il existe certaines matières dans lesquelles vous ne pouvez pas recourir à la médiation ou à l'arbitrage. Il s'agit des questions relevant de l'ordre public, pour lesquelles vous devez toujours vous adresser à un juge.

186. Quels sont les avantages de l'ADR ?

La liberté : lorsque le litige présente une dimension transnationale, l'ADR permet de contourner les difficultés traditionnelles relatives aux questions de compétence juridictionnelle et de loi applicable (*infra*, n^{os} 190 et s.). Les parties peuvent fixer librement le nombre d'arbitres, la possibilité d'un recours, etc.

La flexibilité : cette solution est plus flexible que le recours à la justice traditionnelle. A tout moment, vous pouvez trouver un accord avec votre "adversaire" et arrêter la procédure. Ici, l'implication des parties dans la recherche commune d'une solution au litige est bien plus importante. De plus, le médiateur, conciliateur ou arbitre peut décider non seulement au regard de dispositions légales mais aussi en équité et sur la base de codes de conduite.

La facilité : progressivement, il devient possible de gérer un litige entièrement sur Internet. Vous pouvez remplir un formulaire directement en ligne afin d'introduire une plainte ; ainsi vous ne devez plus vous rendre devant un tribunal. En principe, vous ne devez pas demander à un avocat de s'occuper de votre dossier. Toutefois, il peut être prudent de se faire conseiller par un avocat.

La rapidité : la procédure est généralement rapide et permet donc d'être vite fixé sur l'issue du conflit. Parfois, le simple fait de solliciter l'intervention d'un tiers suffit à régler le problème.

Le prix : le coût est inférieur à celui d'une action en justice. La tendance est de faire payer le coût de la procédure à la société commerciale et de la considérer comme un service au consommateur. Dans cette optique, la procédure est soit gratuite, soit représente des frais modérés pour le consommateur.

La spécificité : un avantage considérable de l'ADR est la possibilité de choisir le tiers. En effet, lorsqu'on a recours aux tribunaux, le juge est imposé et il n'y a aucune garantie que ce dernier soit familiarisé aux nouvelles technologies. Ici, les parties peuvent choisir un spécialiste du domaine qui les concerne.

187. Puis-je me fier à un mécanisme de médiation ou d'arbitrage électronique ?

Nous vous conseillons, avant d'accepter une telle procédure, de vérifier si les conditions suivantes sont respectées : l'indépendance du tiers (arbitre, médiateur ou conciliateur), la transparence de la procédure, la possibilité de vous faire conseiller par un avocat, la sécurité et le prix. En cas de doute, adressez-vous à un avocat pour vous faire conseiller.

Sachez, de manière générale, que le fait pour vous de choisir ces modes de résolution des conflits ne peut vous pénaliser et diminuer vos droits (comme consommateur) par rapport à la protection que vous auriez devant les cours et tribunaux.

188. Peut-on m'imposer lors d'un contrat le recours à ce type de mécanisme ?

Avant la naissance du conflit, vous ne pouvez pas valablement consentir à recourir à l'arbitrage en cas de conflit. Si vous le faites, cette clause sera considérée comme nulle. Une fois que le conflit est né, vous pouvez alors valablement conclure une convention d'arbitrage qui vous oblige (tout comme elle oblige votre "adversaire") à recourir à la procédure d'arbitrage ou de médiation.

Le problème ne se pose pas dans les mêmes termes pour la médiation ou la conciliation pour lesquelles il est possible de prévoir une clause avant la naissance du conflit. En effet, ces modes de résolution des litiges sont moins contraignants.

189. Quelle est la valeur d'une décision d'ADR ?

Vous pouvez toujours agir en justice si la procédure de médiation ou de conciliation n'a pas permis de résoudre le conflit.

Par contre, le recours aux cours et tribunaux n'est plus possible, en principe, si vous vous êtes engagé dans une procédure d'arbitrage. D'une certaine manière, l'arbitrage est la forme la plus achevée des règlements extrajudiciaires de litiges ; en effet, la décision résultant d'un arbitrage s'apparente presque à un jugement des cours et tribunaux et doit donc être respectée.

Partie 6.
La résolution des litiges transnationaux sur Internet

Internet favorise l'établissement de relations par-delà les frontières géographiques. Cette dimension transnationale peut s'avérer problématique lorsque survient un litige. En effet, si vous entendez engager des poursuites judiciaires à l'encontre d'un particulier ou d'une société établis dans un Etat différent du vôtre, vous devrez identifier en premier lieu le tribunal compétent pour connaître de l'affaire et ensuite la loi qui doit régir le litige.

Pour vous aider dans cette tâche, il convient de se tourner vers les règles du droit international privé. En principe, chaque pays dispose de ses propres règles sur la base desquelles sont désignées les juridictions compétentes et les lois applicables. Cependant, une large uniformisation de ces règles a été réalisée au niveau européen grâce à l'adoption d'instruments juridiques internationaux. Afin de déterminer le juge compétent pour connaître du litige, vous pouvez, sans trop d'hésitation, vous référer à un récent Règlement européen, dit "Règlement de Bruxelles". Par contre, les sources juridiques à prendre en considération pour désigner la loi applicable étant plus nombreuses, plusieurs difficultés apparaissent lorsqu'il s'agit de bien comprendre leur articulation. Pour la simplicité, en matière contractuelle, seules seront envisagées les règles applicables lorsque vous contractez en qualité de "consommateur", c'est-à-dire pour un usage étranger à votre activité professionnelle. Les personnes contractant à titre professionnel sont soumises à un autre régime.

Enfin, il ne faut pas perdre de vue que si une décision judiciaire est obtenue en Belgique, encore devra-t-elle pouvoir être exécutée dans le pays où est établie l'autre partie. Il ne suffit donc pas qu'une décision soit rendue dans un Etat pour qu'elle soit exécutoire dans un autre Etat. Cependant, en Europe, le Règlement de Bruxelles rend quasi automatique la reconnaissance et l'exécution des décisions de justice à l'intérieur de l'Union. Par contre, l'exécution en dehors de l'Union européenne d'un jugement obtenu en Belgique pourra s'avérer plus délicate

CHAPITRE I. LA JURIDICTION COMPETENTE EN CAS DE LITIGE TRANSNATIONAL

190. Puis-je poursuivre en Belgique une personne ou une société étrangère ?

De manière générale, en Europe, la juridiction compétente est, en principe, celle de l'Etat où le défendeur (la personne à l'encontre de laquelle l'action en justice est dirigée) a son domicile. Cette solution générale est consacrée dans le Règlement de Bruxelles.

Néanmoins, ce même Règlement prévoit des règles spéciales en matière de contrats conclus par un consommateur et en matière délictuelle.

En matière contractuelle, une option est ouverte à l'intention du consommateur : vous pouvez exercer votre action soit devant les tribunaux belges, soit devant les tribunaux de l'Etat sur le territoire duquel est domiciliée l'autre partie. Pour cela, il faut cependant que les activités professionnelles ou commerciales de votre cocontractant soient exercées dans ou dirigées vers votre pays de résidence. Concrètement, cette condition signifie que si le contrat est conclu sur un site web interactif, accessible depuis votre pays de résidence, vous pourrez bénéficier de ladite option. Grâce à cette règle protectrice, vous pourrez donc agir devant les juridictions belges si vous le souhaitez.

Par contre, le simple fait pour vous d'être informé à propos d'un produit ou d'un service par le biais d'un site "passif" (ne permettant pas de conclure un contrat), accessible dans votre pays de résidence ne suffirait pas. Dans ce cas, vous seriez soumis au même régime que celui des commerçants, en vertu duquel une partie peut être attraite devant le tribunal du

lieu où l'obligation qui sert de base à la demande a été ou doit être exécutée. Plus concrètement, le Règlement fait à cet égard une distinction entre la vente de marchandises et la fourniture de services. Ainsi, le lieu d'exécution de l'obligation qui sert de base à la demande est :

- pour la vente de marchandises, le lieu d'un Etat membre où, en vertu du contrat, les marchandises ont été ou auraient dû être livrées ;

- pour la fourniture de services, le lieu d'un Etat membre où, en vertu du contrat, les services ont été ou auraient dû être fournis.

En matière délictuelle, une option vous est également ouverte. Ainsi, vous pouvez agir en justice, soit dans le pays où le fait générateur du dommage s'est produit, soit dans celui ou le dommage est survenu. On peut en déduire, par exemple, qu'en cas de diffamation sur le web, vous pourrez assigner l'émetteur de l'information qui vous a causé un dommage, soit devant un tribunal situé dans le pays d'où a eu lieu l'émission (le tribunal d'un autre Etat), soit devant le tribunal du lieu où est reçue l'information à l'origine de votre préjudice (le tribunal belge).

191. Puis-je être assigné devant une juridiction étrangère ?

Le Règlement de Bruxelles assure à cet égard une protection du consommateur. L'action intentée à votre encontre ne peut être portée que devant les tribunaux de l'Etat sur le territoire duquel vous êtes domicilié. Pour cela, il faut également que les activités professionnelles ou commerciales de votre cocontractant soient exercées dans ou dirigées vers votre pays de résidence (*supra*, n° 190). Ainsi, en tant que consommateur, vous ne pourrez être assigné en justice que devant les tribunaux belges.

Toutefois, si l'autre partie au contrat n'est pas liée par le Règlement de Bruxelles, vous perdez le bénéfice de cette règle.

192. Peut-on m'imposer la compétence d'une juridiction étrangère lors de la conclusion d'un contrat ?

En règle générale, aucun contrat ne peut avoir pour effet de vous priver, en tant que consommateur, des règles protectrices consacrées par le Règlement de Bruxelles. Ainsi, par exemple, lorsque vous décidez d'acheter un produit sur un site étranger, vous pourrez toujours en cas de problème saisir les tribunaux belges, et cela même si les conditions générales du site prévoient la compétence exclusive des tribunaux du domicile du cyber-vendeur.

CHAPITRE II. LA LOI APPLICABLE EN CAS DE LITIGE TRANSNATIONAL

193. Quels sont les grands principes ?

La détermination de la loi applicable à un litige transnational n'est pas chose aisée ; certains doutes peuvent en effet surgir quant au choix de l'instrument juridique à prendre en considération. Eu égard à la complexité de cette matière, on ne peut que vous encourager à avoir recours aux conseils d'un spécialiste. Toutefois, il n'est pas inutile d'exposer ici les grands principes.

La loi sur le commerce électronique pose le principe selon lequel le juge est tenu d'appliquer la loi d'origine du prestataire, c'est-à-dire la loi du pays où il est établi. Ainsi, dans l'hypothèse d'un conflit entre un prestataire d'hébergement français et une entreprise belge mécontente des services fournis, s'appliquera en principe la loi d'origine du prestataire, c'est-à-dire la loi française.

Cette règle devra toutefois être écartée dans certaines hypothèses, notamment lorsque les parties ont choisi la loi applicable au contrat ou en matière d'obligations contractuelles dans les contrats conclus avec les consommateurs. Pour rappel, comme nous ne traitons ici que des contrats de consommation, nous laisserons de côté les règles de la loi sur le commerce électronique pour nous tourner uniquement vers celles de la Convention de Rome.

Avant d'exposer les solutions proposées par la Convention de Rome, il ne faut pas perdre de vue que deux éléments peuvent avoir une influence significative sur la détermination de la loi applicable : d'une part, les règles protectrices du consommateur (qui jouent à son profit moyennant le respect de certaines conditions), d'autre part, la liberté pour les parties de choisir la loi applicable à leur contrat.

194. La Convention de Rome prévoit-elle des règles protectrices pour le consommateur ?

Oui, mais les règles protectrices prévues par la Convention au bénéfice du consommateur ne vont pouvoir jouer que dans des hypothèses limitativement énumérées. Nous ne nous pencherons ici que sur l'hypothèse la plus générale qui se présente comme une catégorie résiduelle susceptible d'englober la plupart des contrats de consommation. Cette hypothèse impose que la conclusion du contrat ait été précédée dans le pays de la résidence habituelle du consommateur d'une proposition spécialement faite ou de publicité et que le consommateur ait accompli dans ce pays les actes nécessaires à la conclusion du contrat.

En posant cette exigence d'une proposition ou d'une publicité dirigée vers le pays du consommateur, la Convention de Rome tend à opérer une distinction entre consommateurs "actifs" et "passifs", en ne permettant l'application des règles protectrices qu'au profit du consommateur dit "passif". Toutefois, une telle distinction suscite plusieurs difficultés au regard des situations contractuelles nées de l'utilisation d'Internet.

Certains cas de figure ne poseront pas de grandes difficultés. En effet, on peut aisément admettre qu'une certaine passivité sera de mise en cas de proposition individualisée ou encore chaque fois que la publicité par laquelle vous avez été sollicité était personnalisée. On sait en effet que la collecte des données personnelles relatives aux internautes et leur centralisation dans des bases de données permettent de dégager des profils de

consommation autorisant une véritable personnalisation de la publicité (*supra*, n^{os} 63 et s.).

D'autres cas s'avéreront nettement plus problématiques. Vous pouvez notamment, en cours de navigation, repérer un site présentant une base de données ou des biens à acquérir et vous identifier auprès du responsable du site pour bénéficier du service proposé et ce, sans jamais avoir été sollicité par le commerçant. Vous pouvez également, en cours de navigation, être attiré par une bannière publicitaire. L'interactivité inhérente à Internet – qui se manifeste notamment par la diversité des techniques publicitaires utilisées – contribue à obscurcir la distinction entre consommateurs actifs et passifs. Le comportement de tout internaute se révèle, en effet, d'une nature ambivalente. Le consommateur qui navigue sur le *net* est "actif" puisqu'il prend l'initiative de se connecter mais il est également soumis, au cours de sa navigation, à diverses formes de sollicitation qu'il ne contrôle pas ou dont il ne soupçonne pas l'influence.

Dans l'attente d'une modification du texte de la Convention de Rome, une difficulté d'interprétation majeure se pose inévitablement au juge.

195. Puis-je "négocier" la loi applicable au contrat ?

Les règles de droit international privé consacrent la liberté des parties de choisir la loi applicable à leur contrat. Il est donc, en principe, possible de négocier.

Très souvent cependant, la loi applicable est désignée par les conditions générales présentes sur le site, sans qu'il soit possible d'en négocier les termes. Ainsi, si vous faites un achat sur un site étranger, la loi applicable sera probablement celle que le vendeur a intérêt à voir appliquer, c'est-à-dire celle de son pays.

La mention de la loi applicable dans les conditions générales présente l'avantage d'une certaine transparence. Toutefois, elle ne va pas résoudre les problèmes qui peuvent survenir si la loi applicable est celle d'un pays tiers qui ne vous offre pas les mêmes garanties de protection que la loi belge. Par exemple, le droit de renonciation pourrait ne pas être prévu par certaines législations étrangères, du moins en dehors de l'Union européenne (*supra*, n^{os} 144 et s.).

Commençons par l'hypothèse où les règles protectrices évoquées précédemment s'appliquent. Il est prévu que la liberté des parties de choisir le droit applicable ne peut avoir pour résultat de priver le consommateur de "*la protection que lui assurent les dispositions impératives de la loi du pays dans lequel il a sa résidence habituelle*". L'on range notamment, parmi ces "dispositions impératives", la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur. L'objectif poursuivi par cette règle est de garantir au consommateur la protection à laquelle il est habitué dans son Etat de résidence. L'application des dispositions protectrices de la loi du consommateur vise donc à empêcher toute tentative des professionnels de s'affranchir, en recourant au choix d'une loi étrangère, de tout ou partie des règles nationales élaborées pour la protection du consommateur. Ainsi, lorsque vous contractez en tant que consommateur dans les conditions fixées par la Convention (*supra*, n° 194) vous pouvez avoir la certitude que vous bénéficierez, au minimum, des mesures spécifiques de protection prévues par les lois impératives belges.

Toutefois, si ces règles protectrices ne peuvent s'appliquer (parce que les conditions décrites plus haut ne sont pas réunies), le contrat sera régi par la loi choisie par les parties ; cependant, le juge saisi peut toujours appliquer ses règles nationales impératives.

196. Quelle est la loi applicable à défaut de choix par les parties ?

A défaut de choix, le contrat est régi par la *loi du pays dans lequel le consommateur a sa résidence habituelle* si ce contrat est intervenu dans les circonstances décrites plus haut, c'est-à-dire notamment lorsque la conclusion du contrat a été précédée dans le pays de la résidence habituelle du consommateur d'une proposition spécialement faite ou de publicité et que le consommateur a accompli dans ce pays les actes nécessaires à la conclusion du contrat.

Toutefois, si les règles protectrices ne peuvent s'appliquer, la Convention de Rome prévoit que le contrat est régi par la loi du pays avec lequel il présente les liens les plus étroits. On présume à cet égard que le contrat présente les liens les plus étroits avec le pays dans lequel la partie qui doit fournir la prestation caractéristique a sa résidence habituelle ou son principal établissement. Par exemple, si vous achetez un livre sur un site français et que, pour une raison ou pour une autre, vous désirez agir en justice contre le vendeur, la loi applicable sera la loi française car la prestation caractéristique est, en l'espèce, la livraison du livre et que le débiteur de cette obligation (le vendeur) a son principal établissement en France. Notez que même dans ce cas, le juge saisi pourra appliquer les dispositions impératives de sa loi nationale.

197. Quelle est la loi applicable en cas de délit ?

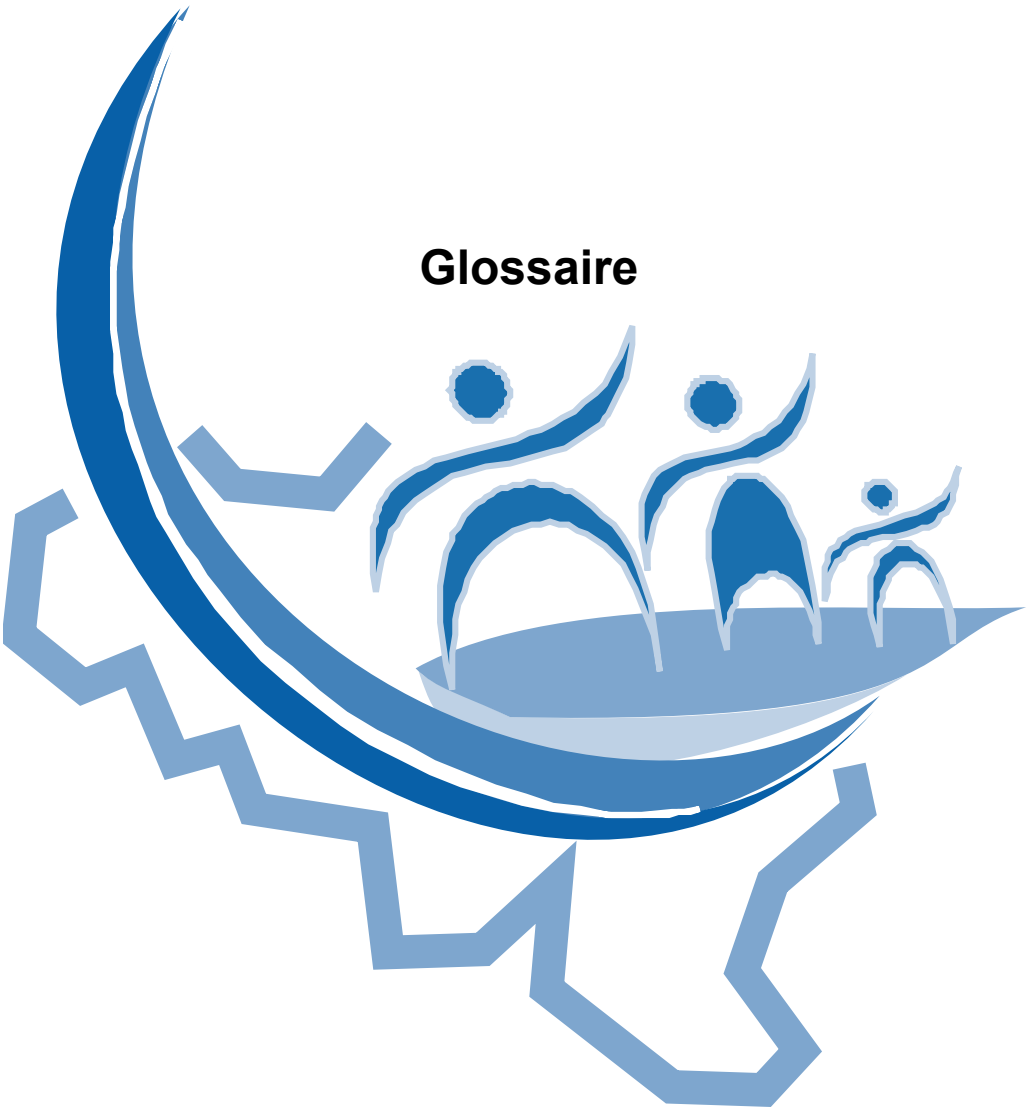
Le recours à l'action en responsabilité délictuelle peut être envisagé dans différentes hypothèses : par exemple, afin de sanctionner une publicité illicite, des propos diffamatoires ou incitant à la haine raciale, etc.

Dans cette matière, vous devez savoir qu'aucune convention internationale n'a été adoptée à ce jour. Toutefois, on peut s'appuyer aujourd'hui sur la législation relative au commerce électronique pour résoudre la question de la loi applicable à un délit commis sur Internet. Pour rappel, cette législation repose sur le principe dit "du pays d'origine", en vertu duquel l'activité de tout prestataire qui fournit un service en ligne est soumise à la loi du pays où il est établi. Chaque fois donc qu'un prestataire commet un délit sur Internet, c'est cette loi qui trouve à s'appliquer.

Il se peut cependant que votre action en responsabilité ne soit pas dirigée contre un prestataire, mais contre un simple particulier qui, par exemple, tient des propos diffamatoires sur un forum de discussion. La détermination de la loi applicable à une telle action en réparation doit alors se faire sur la base des règles traditionnelles de droit international privé. A cet effet, il faut d'abord identifier les juridictions nationales susceptibles de connaître de l'action, étant entendu que chaque juridiction est liée par les seules règles de désignation du droit national applicable qui ont force obligatoire dans son Etat !

Les solutions en matière de droit applicable vont donc varier selon les Etats. De manière générale, la loi la plus souvent désignée dans la plupart des pays européens est celle du lieu de commission du délit. La localisation du lieu de commission d'un délit n'est cependant pas chose aisée sur Internet. Face à cette difficulté, les solutions de la jurisprudence peuvent varier ; les juges retiendront tantôt la loi du pays où s'est produit le fait dommageable, tantôt la loi du pays où s'est réalisé le dommage.

Glossaire



GLOSSAIRE

A

ADR

Alternative Dispute Resolution. Mécanisme visant à résoudre les conflits (en ligne) par des voies alternatives à celles des cours et tribunaux, notamment par le recours à la médiation, la conciliation ou l'arbitrage.

Adresse IP

Adresse *Internet Protocol*, attribuée à chaque ordinateur connecté à Internet et permettant de l'identifier de manière unique. Une adresse IP se présente sous la forme de quatre groupes de chiffres, séparés par des points, par exemple 193.190.127.2.

ADSL

Asymmetric Digital Subscriber Line. Technologie de transmission de données permettant une connexion à haut débit. L'ADSL utilise une ligne téléphonique classique (une paire de fils de cuivre), mais sur des fréquences plus élevées, grâce à un modem de nouvelle génération, ce qui permet de surfer et de rester connecté à Internet en permanence, tout en laissant la ligne téléphonique libre. Les vitesses de transmission sont sensiblement accrues par rapport aux connexions avec un modem classique : de l'ordre de 10 fois plus rapide pour le téléchargement de données et de 2 fois pour l'envoi de données.

Annuaire

L'annuaire (ou répertoire ou index) est un instrument de recherche et de classification de l'information sur Internet. Un annuaire se présente généralement sous la forme de listes de sites, organisées en catégories et sous-catégories, en fonction de leur thème (p. ex., informatique, sciences, santé, sports et loisirs, culture, etc.).

Applet

APPlication Light wEighT. Petit programme informatique écrit en langage Java. Les *applets* sont des applications souvent intégrées dans une page web pour la rendre plus attrayante ou interactive (p. ex., menus déroulants, texte clignotant ou défilant, etc.). Elles ne peuvent être exécutées que si le navigateur web de l'internaute est compatible avec Java. Si une page web contient des *applets*, elle sera généralement plus longue à télécharger.

B

Bannière ou bandeau

Espace d'expression publicitaire (souvent de petite taille) occupant une partie de la page web.

Bande passante

Débit d'une ligne de transmission, correspondant au volume de données pouvant être transmises en un laps de temps donné. La bande passante se mesure généralement en bits par seconde (bps). Plus la bande passante est large, plus le volume potentiel d'informations qui transitent par unité de temps est important.

Baud

Unité mesurant la rapidité de modulation. Souvent confondu avec le bit par seconde (bps). En général, un baud est équivalent à un bit par seconde, mais cela dépend de la valence du signal (c'est-à-dire le nombre de valeurs différentes qu'il peut prendre). Dans les modems actuels, un baud vaut plusieurs bps.

Voir aussi "Modem" et "Bps".

Bit

BInary digiT. Il s'agit de la plus petite unité du langage informatique, qui peut prendre deux valeurs : 1 ou 0. A partir d'un regroupement de bits on peut former des codes pour représenter des caractères, des nombres, ou tout type d'information. Ainsi, il faut 8 bits pour former un caractère. Ce groupement de 8 bits est appelé *byte* ou octet.

Bit par seconde (ou bps ou bit/s)

Unité de mesure d'un débit de transmission sur les réseaux. Voir aussi "Bande passante".

Byte

Voir "Octet".

Browser

Voir "Navigateur".

***Bug* ou bogue**

Un *bug* est une erreur de programmation entraînant un fonctionnement défectueux du programme.

C

Certificat numérique

Un certificat numérique est une attestation électronique, délivrée par un prestataire de service de certification, qui lie une personne physique ou morale à sa clé publique et confirme l'identité de cette personne. Le lien est certifié par le certificat signé par cette autorité de certification. Cette signature prouve l'authenticité du certificat et empêche toute modification des informations qu'il contient.

Chat

Conversation en ligne, en temps réel, entre plusieurs usagers d'Internet échangeant des messages écrits.

Chiffrement ou cryptage

Opération permettant de protéger la confidentialité de données, par le recours à des clés (mots de passe, code secret…) qui encodent les informations en les traduisant sous forme de chiffres, de telle sorte que seul le détenteur de ces clés peut lire l'information ainsi protégée.

Client-serveur

Architecture ou mode de fonctionnement de plusieurs ordinateurs connectés en réseau, où un programme d'application appelé "client" fait appel à différentes ressources localisées sur d'autres machines du réseau appelées "serveur". Les machines s'échangent ainsi des services par l'intermédiaire de requêtes et de réponses.

Commission de la protection de la vie privée

Institution servant de point de contact et d'organe consultatif en matière de protection de la vie privée et des données à caractère personnel.

Consortium W3 (ou W3C)

World Wide Web Consortium (www.w3.org). Organisation qui élabore des standards pour le web et favorise l'interopérabilité des produits du *World Wide Web*.

Contrat à distance

Tout contrat concernant des produits ou des services conclu entre un vendeur et un consommateur dans le cadre d'un système de vente ou de prestations de services à distance organisé par le vendeur qui, pour ce contrat, utilise exclusivement une ou plusieurs techniques de communication à distance jusqu'à la conclusion du contrat, y compris la conclusion du contrat elle-même (article 77 § 1er, 1°, loi sur les pratiques du commerce et sur la protection et l'information du consommateur).

Cookie

Petit fichier informatique au format texte, envoyé par un serveur web lors de la consultation d'un site, et stocké sur le disque dur de l'ordinateur de l'internaute. Il contient des données réutilisées à chaque consultation du même site, pour identifier l'ordinateur ou les préférences de l'utilisateur.

Courrier électronique (ou *e-mail* ou courriel)

Tout message sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communications, qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier en prenne connaissance.

***Cybersquatting* (ou *Domain name grabbing* ou usurpation de nom de domaine)**

Pratique consistant à faire enregistrer un nom de domaine correspondant à une marque, un nom commercial, un nom patronymique, dans le but d'empêcher le titulaire de cette marque ou de ce nom d'enregistrer ce nom de domaine, ou afin de le lui revendre au prix fort.

D

DNS

Domain Name System. Système permettant de traduire une URL (de type www.site.com) en une adresse IP (p. ex. 193.190.127.2).

Voir aussi "URL" et "Adresse IP".

Domain name grabbing

Voir "*Cybersquatting*".

Donnée à caractère personnel

Toute information concernant une personne physique identifiée ou identifiable. Une personne est identifiable lorsqu'elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

Droit de renonciation

Possibilité offerte au consommateur, dans le cadre d'un contrat à distance, de renoncer à son achat, sans pénalités ni indication de motifs.

Droit international privé

Ensemble de règles de droit permettant, en cas de litige transnational, de déterminer quelles sont la juridiction compétente et la loi applicable.

E

e-mail

Voir "Courrier électronique".

Espiogiciel (ou *spyware*)

Mouchard électronique prenant la forme d'un petit programme intégré à un logiciel (p. ex. certains *freewares* ou *sharewares* téléchargés sur Internet) et qui collecte des données relatives à un internaute, à son itinéraire sur le web et à la configuration de sa machine. Lors de chaque connexion à Internet, ces informations sont envoyées sur un serveur, généralement afin d'adresser à l'internaute des publicités ciblées.

F

FAQ (ou *Frequently Asked Questions* ou Foire Aux Questions)

Liste de réponses aux questions les plus fréquemment posées par les internautes au sujet du site ou des termes qu'il aborde.

Faux en informatique

Manipulation informatique de données afin de modifier intentionnellement leur portée juridique. Des données électroniques peuvent être ainsi falsifiées moyennant modification ou effacement (complet ou partiel) lors de leur saisie (introduction dans l'ordinateur), de leur récupération ou au cours de leur stockage. Constituent des faux en informatique, notamment : la confection illégale ou la falsification de cartes de crédit ; les faux en matière de contrats numériques (lorsque les données juridiquement pertinentes ne sont plus imprimées sur papier, ni signées à l'aide de la main) ; l'introduction d'un faux numéro de carte de crédit lors de l'inscription à un site Internet payant ; l'inscription de créances fictives ou la modification de données salariales par un employé dans le logiciel comptable de l'entreprise ; le fait, pour un employé, de gonfler artificiellement les heures supplémentaires encodées dans le logiciel de gestion du temps de travail ; la falsification d'une signature électronique ou encore l'utilisation en pleine connaissance de cause de données falsifiées.

Filtrage

Système composé d'un ou de plusieurs logiciels visant à empêcher les utilisateurs d'Internet d'accéder à certains contenus qu'ils jugent inappropriés, notamment pour leurs enfants. Les filtres peuvent également servir pour éviter de recevoir des publicités non sollicitées par courrier électronique.

***Firewall* (ou pare-feu)**

Dispositif matériel et logiciel destiné à interdire tout accès non autorisé à un réseau informatique.

Flame

Message de réprimande envoyé par les internautes à l'encontre de celui qui tient des propos inacceptables sur un forum de discussion.

Forums de discussion (ou *newsgroup*)

Lieu de discussion interactif où les utilisateurs peuvent échanger des informations, idées, astuces, conseils et opinions sur un thème particulier. Contrairement au *chat*, les messages ne circulent pas en temps réel, mais en différé. Les utilisateurs peuvent lire tous les messages rédigés par d'autres abonnés du forum et leur répondre soit collectivement, soit individuellement.

Fournisseur d'accès à Internet (FAI) ou *Internet Service Provider* (ISP)

Intermédiaire permettant aux particuliers et aux entreprises de se connecter au réseau Internet.

Framing

Pratique consistant à afficher une page ou un contenu provenant d'un autre site (site source) dans sa propre page web (site cible), sans passer par l'ouverture d'une nouvelle fenêtre du navigateur renvoyant au site source. L'adresse du site cible est donc substituée à celle du site source, ce qui donne la fausse impression que le contenu en question est celui du site cible.

Fraude informatique

Manipulation illicite de données électroniques afin d'en retirer un avantage patrimonial frauduleux. Constituent des fraudes informatiques, par exemple, l'utilisation d'une carte de crédit volée pour retirer de l'argent d'un distributeur automatique de billets, le dépassement illicite du crédit octroyé par sa propre carte de crédit, l'introduction d'instructions de programmation permettant d'obtenir à la suite de certaines transactions d'autres résultats en vue d'un avantage financier illicite, ou encore les manipulations illégitimes effectuées par un employé de banque sur les comptes des clients.

Freeware

Logiciel disponible gratuitement. A ne pas confondre avec le *shareware*.

FTP ou *File Transfer Protocol*

Protocole de transfert de fichiers sur Internet.

G

GIF

Graphics Interchange Format (format d'échange graphique). Type de format de fichier graphique destiné aux documents du *World Wide Web*.

H

Hacking

Accès non autorisé au système informatique d'un tiers ou fait de s'y maintenir (*hacking* externe). Le *hacking* peut également consister dans le fait d'outrepasser son pouvoir d'accès à ce système (*hacking* interne).

Hardware

Matériel informatique. *Hardware* s'oppose à *software*, qui désigne le logiciel.

Hébergeur ou prestataire d'hébergement

Opérateur technique sur Internet qui fournit un espace pour stocker un site web et le rendre consultable.

Helpdesk* ou *hotline

Assistance téléphonique (gratuite ou payante) mise en place par un professionnel afin de répondre aux questions de ses clients.

Hoax

Message de fausse information, canular circulant sur Internet, souvent par le biais du courrier électronique.

HTML

HyperText Markup Language. Langage permettant la création et la description de pages web (documents hypertextes) sur Internet.

HTTP

HyperText Transfer Protocol (protocole de transfert de lien hypertexte). Protocole de base de la technologie du *World Wide Web*, gérant les communications entre ordinateurs sur Internet.

Hypertexte

Mode de présentation des informations sur Internet permettant de lier des images, des sons et du texte de façon à pouvoir consulter ces contenus indépendamment de leur localisation et de leur support. Voir aussi "Lien hypertexte".

I

ICANN

Internet Corporation for Assigned Names and Numbers. Organisation représentative de l'ensemble des acteurs et utilisateurs d'Internet, dont la fonction consiste à coordonner la gestion du système des noms de domaine, de l'adressage IP, des paramètres du protocole IP ainsi que du serveur "root".

Interface

Jonction entre deux opérateurs (matériel, logiciel, humain) leur permettant d'échanger des informations par l'adoption de règles communes, physiques ou logiques.

Internaute

Utilisateur d'Internet.

Internet

Réseau mondial, composé d'un ensemble de réseaux plus petits, par lequel des ordinateurs situés aux quatre coins du monde peuvent entrer en communication par l'utilisation d'un protocole commun (TCP/IP). Les services les plus courants sont le *world wide web*, le courrier électronique, les forums de discussion et le transfert de données.

Intranet

Réseau privé interne à une organisation. Les réseaux intranet utilisent fréquemment les protocoles Internet pour livrer leur contenu. Ils sont souvent protégés du réseau Internet par des *firewalls* (ou pare-feu).

IP

Internet Protocol : protocole utilisé sur Internet pour la transmission des données découpées en paquets.

ISDN

Integrated Services Digital Network. Voir "RNIS".

ISP

Internet Service Provider. Voir "Fournisseur d'accès à Internet".

J

Java

Langage de programmation orienté-objet développé par la société *Sun Microsystems* et par IBM, grâce auquel les programmeurs peuvent créer des applications autonomes et interactives spécialement conçues pour Internet. Le programme Java est écrit en texte source puis traduit par un compilateur pour générer un programme appelé *applet* utilisable sur une page HTML. Si vous affichez une page comportant un *applet* Java, à l'aide d'un navigateur prenant en charge le langage Java, le code de l'*applet* sera alors transféré vers votre système et exécuté par le navigateur.

JPEG

Joint Picture Expert Group. Format de compression des images très utilisé sur Internet. Voir aussi GIF.

L

Lien hypertexte

Zone réactive dans un document web. Il peut s'agir d'un mot du texte, différencié du reste du document par sa couleur ou d'une image active. Lorsque l'on clique sur un lien hypertexte, celui-ci renvoie au document désigné par le lien, situé sur la même page web, ou sur une autre page web, appartenant au même site web ou à un autre. Voir aussi "Hypertexte".

Liste Robinson

Liste sur laquelle peut s'inscrire toute personne ne souhaitant plus recevoir des publicités de la part de sociétés dont elle n'est pas cliente ou auxquelles elle n'a pas demandé d'informations. Ces listes existent pour tous les moyens de communication, qu'il s'agisse d'Internet (pour le courrier électronique) ou des téléphones portables (pour les SMS).

Logiciel à contribution volontaire ou *Shareware*

Logiciel disponible pour un essai gratuit, mais pour lequel l'auteur ou le développeur exige une contribution en cas d'utilisation. En général, de tels logiciels sont développés par des petites entreprises ou des programmeurs individuels ayant entrepris de résoudre un problème informatique particulier ou de développer une nouvelle application. En échange de votre contribution, vous recevrez la documentation correspondant au logiciel, des mises à jour régulières...

Login

Nom d'utilisateur ou numéro d'identification pour s'identifier sur un serveur. Il est généralement accompagné d'un mot de passe.

M

Métatag

Sorte de balise placée dans l'entête d'une page HTML, fournissant une description d'un site par le biais de mots-clés, afin que ce site soit référencé au mieux par les moteurs de recherche.

Modérateur

Personne chargée de la gestion d'un forum de discussion ou d'une liste de diffusion et dont le rôle consiste à filtrer les messages envoyés par les participants en écartant ceux qui se révèlent hors sujet ou dont le contenu dépasse les limites éthiques ou déontologiques fixées.

Modem

Acronyme de MOdulateur/DEModulateur. Elément périphérique d'un ordinateur par lequel celui-ci est relié à un réseau, le plus souvent Internet, par le biais de la ligne téléphonique ou du câble de télédistribution. Un modem peut être interne (intégré à un ordinateur) ou

externe. Les différents modems se distinguent par leur vitesse de transmission des données (exprimée en bauds) et la technologie de télécommunication choisie (ADSL, RNIS, etc.).

Moteur de recherche

Programme ou service utilisé pour localiser des informations sur le web. Chaque moteur de recherche utilise un logiciel d'exploitation qui balaie les pages web et les indexe dans une base de données. A la requête de l'internaute, le moteur de recherche affichera une série de documents hypertextualisés correspondant au mot-clé soumis. Les moteurs de recherche les plus connus sont Google, Alta Vista, Lycos, Yahoo !

MP3

Mep-1 Layer 3. Format de fichier audio permettant d'assurer une qualité d'écoute comparable à celle d'un CD Audio et un taux de compression allant jusqu'à 13.

Multimédia

Terme désignant tout contenu qui combine du texte, des graphiques, des fichiers son et/ou vidéo.

N

Navigateur

Logiciel permettant à l'internaute de rechercher des informations sur Internet et de les consulter. Les plus connus sont Netscape Navigator et Internet Explorer.

Net

Terme utilisé familièrement pour désigner Internet.

Nétiquette

Ensemble des règles de savoir-vivre et de bonne conduite sur Internet.

Nom de domaine

Correspondant plus convivial et facilement mémorisable de l'adresse IP qui permet l'identification d'un ordinateur ou d'un groupe d'ordinateurs sur Internet. Le nom de domaine comprend deux parties majeures : le radical et l'extension, la première reprenant généralement le nom de l'organisation et la seconde faisant référence au rattachement géographique de celle-ci (.be, .fr, .uk, etc.) ou à son type d'activité (.com, .org, .net, etc.). Par exemple, le nom de domaine de la Chambre des Représentants de Belgique est "lachambre.be".

O

Octet ou *byte*

Ensemble de 8 bits permettant d'obtenir 256 possibilités (2^8), chaque bit pouvant représenter un 1 ou un 0. Un exemple d'octet est 01001010. Un mégaoctet correspond à un million d'octets.

P

Page d'accueil (ou *Home page*)

Page principale d'un site web. Les pages d'accueil contiennent généralement des liens qui renvoient à d'autres emplacements du site propre ou de sites externes. Certains sites web de grande taille peuvent posséder plusieurs pages d'accueil.

PDF

Portable Document Format. Format de fichiers créé par Adobe qui compresse ceux-ci pour en réduire la taille (jusqu'à 10 fois) et qui permet de visualiser et d'imprimer les données sur n'importe quelle plate-forme via l'outil Acrobat Reader.

PIN

Personal Identification Number. Code secret personnel.

Plate-forme

Matériel et logiciel système sur lesquels repose un système informatique.

Plug-in

Composant ou module logiciel qui améliore les capacités d'une application, généralement pour permettre de lire ou d'afficher des fichiers d'un type particulier. Dans le cas du navigateur web, les *plug-in* servent à afficher du contenu riche, tels que des fichiers audio, vidéo ou des animations.

Pop-up

Fenêtre de navigation qui s'ouvre au-dessus de la fenêtre principale. De nombreux sites affichent des publicités dans de telles fenêtres.

Portail

Site Internet fédérateur à partir duquel l'utilisateur commence sa recherche. Il propose généralement des services variés, tels la gestion d'une adresse e-mail, des informations d'actualité, des annuaires… Parmi les plus répandus, on peut citer Yahoo !, Belgacom ou Advalvas.

Prestataire de service de certification (PSC)

Le prestataire de service de certification est un organisme indépendant habilité, d'une part, à *vérifier l'identité* des titulaires de clé publique et à *générer des certificats*, sortes d'attestations électroniques qui font le lien entre une personne et sa clé publique, et, d'autre part, à *assurer la publicité* la plus large des certificats ainsi émis. Le PSC est également tenu de maintenir à jour le répertoire contenant les certificats de clé publique, en

veillant le cas échéant, à leur révocation. En guise d'exemple, Belgacom E-Trust, Globalsign et Isabel sont des prestataires de service de certification.

Protocole

Ensemble de règles ou standards établis pour la communication des données sur un réseau, en particulier Internet. Les ordinateurs communiquent par le biais de protocoles qui déterminent leur comportement mutuel pour que le transfert des informations puisse s'effectuer. Sur Internet, le protocole de référence est le TCP/IP.

Provider

Voir "Fournisseur d'accès à Internet".

R

Recommandé électronique

A l'instar du recommandé traditionnel, le recommandé électronique permet à l'expéditeur d'un message signé électroniquement de se constituer une preuve de l'envoi, de la date, et le cas échéant, de la réception, grâce à l'intervention d'un tiers de confiance.

RNIS ou ISDN

Réseau Numérique à Intégration de Services - *Integrated Services Digital Network* (ISDN). Réseau entièrement numérisé permettant un transfert rapide et fluide d'informations. Il existe deux types de lignes ISDN : l'ISDN-2, muni de deux canaux de communication de 64.000 bits par seconde chacun et l'ISDN-30, muni de trente canaux de communication.

Routeur

Equipement servant à connecter un ou plusieurs réseaux en offrant la possibilité de filtrer et de diriger un signal en fonction de son adresse IP.

S

***Script* ou langage script**

Ensemble de commandes grâce auxquelles les différentes tâches d'un programme de communication sont automatisées.

Serveur

Ordinateur, ou son logiciel, inséré dans un réseau et capable d'offrir certains services aux autres ordinateurs du réseau, considérés comme ses clients.

SET

Secure Electronic Transactions. Protocole de sécurisation de paiements électroniques basé sur une technologie de cryptage et permettant l'authentification des parties.

SMTP

Simple Message Transfer Protocol. Protocole de communication TCP/IP utilisé pour l'envoi de courriers électroniques sur Internet.

Site web

Ensemble de pages web reliées, résidant sur le même serveur et interconnectées par des liens hypertexte.

Software

Logiciel informatique. Voir aussi "*Hardware*".

Spamming

Envoi massif et répété, de messages non sollicités, le plus souvent à caractère commercial.

Spyware

Voir "Espiogiciel".

SSL

Secure Socket Layer. Protocole de communication cryptée via Internet, intégré dans les logiciels de navigation (Netscape Navigator et Internet Explorer), utilisé pour sécuriser les transferts de données confidentielles sur les réseaux.

Streaming

Technique permettant de lire un fichier (image, fichier audio ou vidéo) sans devoir attendre son téléchargement complet. Un *plug-in* ajouté au navigateur Web décompresse et lit les données au fur et à mesure de leur arrivée sur l'ordinateur.

T

TCP/IP

Combinaison des acronymes de *Transmission Control Protocol* (protocole de contrôle de transmission) et de *Internet Protocol* (protocole Internet), les deux protocoles de communication à la base du fonctionnement d'Internet et régissant les transferts d'informations sur les réseaux.

Téléchargement ou *downloading*

Procédure visant à demander et à transférer un fichier d'un ordinateur distant vers un ordinateur local, puis à sauvegarder ce fichier dans l'ordinateur local.

Traitement de données à caractère personnel

Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel. Il peut consister, notamment, en la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la consultation, l'utilisation, la diffusion… de données.

Voir aussi "Donnée à caractère personnel".

U

URL

Uniform Resource Locator (localisateur uniforme de ressources). Adresse d'un serveur ou de toute ressource disponible sur Internet. La première partie de l'URL désigne le protocole (http ou ftp), ensuite vient le nom du domaine ou l'adresse IP (www.lachambre.be ou 212.35.105.232), puis éventuellement un ou plusieurs répertoires permettant d'accéder à la ressource sur le serveur.

Par exemple : http://www.lachambre.be/documents_parlementaires.html.

V

Virus

Programme destiné à perturber le fonctionnement des systèmes informatiques ou à modifier, corrompre, voire détruire, les données qui y sont stockées. Capable de se reproduire de lui-même, le virus est conçu pour détecter d'autres programmes et les infecter en leur incorporant sa propre copie. L'activation du virus s'opère au moment où le programme infecté est exécuté. Une fois activé, le virus commence à produire ses effets, qui peuvent s'avérer simplement gênants ou incommodants mais aussi désastreux, voire franchement catastrophiques.

W

le Web

Abréviation de *World Wide Web*.

***World Wide Web* (ou www ou web)**

Ensemble de systèmes informatiques (serveurs web) connectés à Internet et utilisant des normes communes (les techniques d'hypertexte) pour diffuser des pages d'informations multimédias (pages web).

W3C

Voir "Consortium W3".

Textes et adresses utiles

TEXTES UTILES

Protection du consommateur

- Loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur, *M.B.,* 29 août 1991.

Protection de la vie privée

- Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993.

- Arrêté royal du 13 février portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 13 mars 2001.

Droits d'auteur et droit des marques

- Loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins, *M.B.,* 27 juillet 1994, pp.19297-19314.

- Loi du 30 juin 1994 transposant la directive européenne du 14 mai 1991 sur la protection juridique des programmes d'ordinateur, *M.B.,* 27 juillet 1994, pp. 19315-19317.

- Loi du 31 août 1998 transposant la directive européenne du 11 mars 1996 concernant la protection juridique des bases de données, *M.B.,* 14 novembre 1998, p. 36914.

- Loi du 30 juin 1969 portant approbation de la Convention Benelux en matière de marques de produits, et annexe, signée à Bruxelles le 19 mars 1962, *M.B.*, 14 octobre 1969. Cette loi uniforme Benelux a été modifiée à plusieurs reprises. La dernière en date est la loi du 3 juin 1999 portant assentiment au Protocole portant modification de la loi uniforme Benelux sur les marques, fait à Bruxelles le 7 août 1996, *M.B.*, le 26 octobre 1999.

Commerce électronique

- Loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *M.B.,* 17 mars 2003.

- Loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, *M.B.*, 22 décembre 2000.

- Loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, *M.B.*, 29 septembre 2001.

- Loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds, *M.B.*, 17 août 2002.

Criminalité informatique

- Loi du 13 avril 1995 contenant des dispositions en vue de la répression de la traite des êtres humains et de la pornographie enfantine, *M.B.*, 25 avril 1995, p. 10823.

- Loi du 28 novembre 2000 sur la criminalité informatique, *M.B.*, 3 février 2001.

Droit international privé

- Règlement (CE) n° 44/2001 du Conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, *J.O.C.E.*, n° L 12/1, 16 janvier 2001.

- Convention de Rome du 19 juin 1980 sur la loi applicable aux obligations contractuelles, *J.O.C.E.*, n° L 266/1, 9 octobre 1980.

ADRESSES UTILES

- Site du **Service public fédéral Economie, PME, Classes moyennes et Energie** :

  http://mineco.fgov.be

- **Administration du Contrôle et Médiation**: pour adresser une plainte :

  World Trade Centre III

  Boulevard Simon Bolivar, 30

  1000 Bruxelles

  Tél. : 32 (0) 2 208 36 11

  Fax : 32 (0) 2 208 39 15

  E-mail : Eco.Inspec@mineco.fgov.be

- Site de l'**Observatoire des Droits de l'Internet :**

  http://www.Internet-observatory.be

- **Strategisch Digitaal Forum :**

  http://www.eflanders.be

- Agence **Wallonne des Télécommunications :**

  http://www.awt.be

- **Etat fédéral, Communautés et Régions : portails institutionnels**

http://www.belgium.be	Etat fédéral
http://www.cfwb.be	Communauté française
http://www.vlaanderen.be	Communauté flamande (Région flamande)
http://www.dglive.be	Communauté germanophone
http://www.wallonie.be/	Région wallonne
http://www.bruxelles.irisnet.be	Région de Bruxelles-Capitale

- **Point de contact de la police judiciaire** : pour dénoncer un contenu illicite sur Internet

  E-mail : contact@gpj.be

- ***Child Focus :***

  Tél. : 110

  www.childfocus-net-alert.be

- Site de la **Commission de la Protection de la Vie privée** :

  http://www.privacy.fgov.be

- Site **Interdisciplinair Centrum voor Recht en Informatica**

  http://www.icri.be

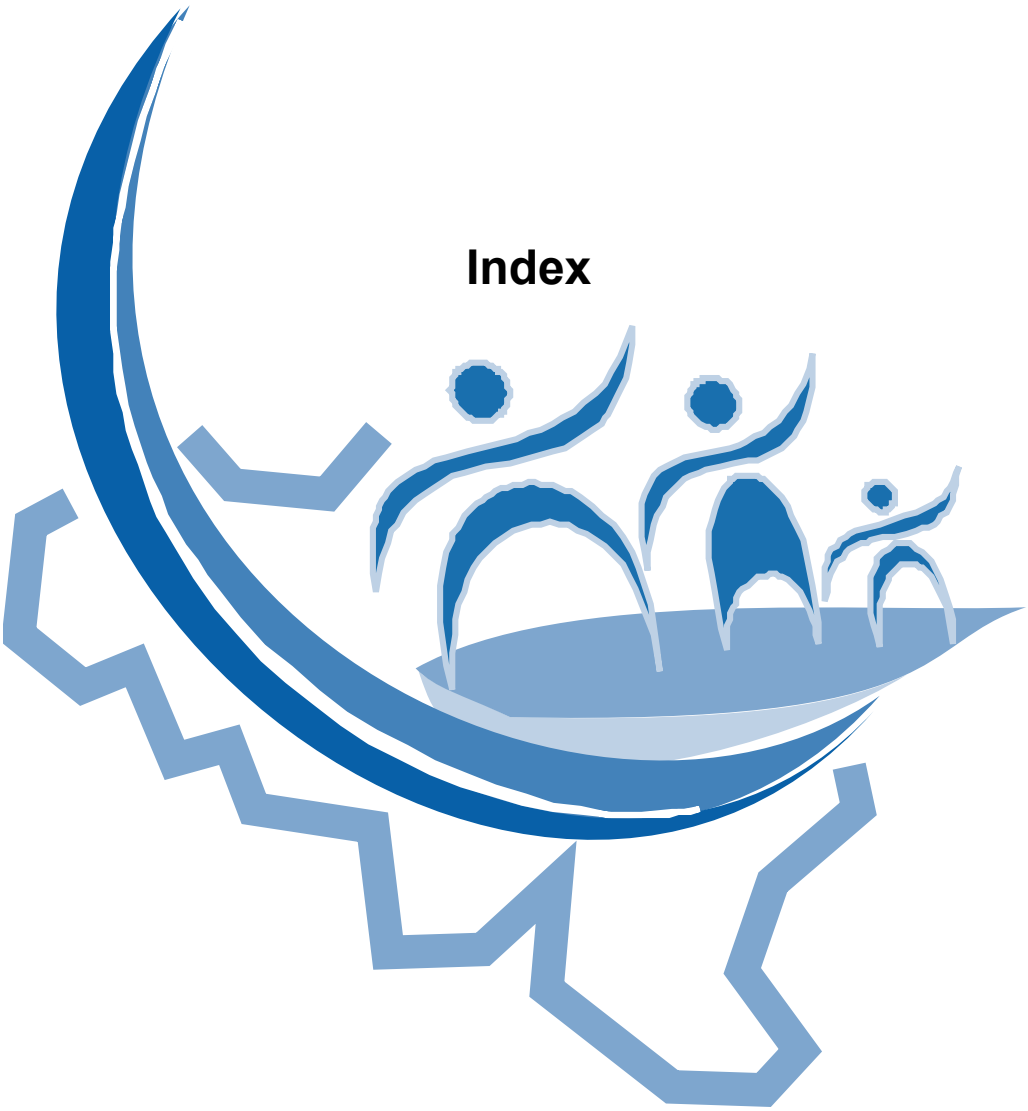
- Site du **Centre de Recherches Informatique et Droit** :

  http://www.crid.be

- ASBL **"Droit et Nouvelles Technologies"** :

  http://www.droit-technologie.org

Index



INDEX

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W